Jyrki Kivimäki

Windows Server NT 4.0

Tehokäyttäjän opas

***Suomen Atk**-kustannus*

Windows NT 4.0 – tehokäyttäjän opas

Kaikki oikeudet pidätetään. Tämän julkaisun jäljentäminen ilman tekijän kirjallista lupaa painamalla, monistamalla, äänittämällä tai muulla tavoin on tekijänoikeuslain mukaisesti kielletty.

Kirjoittaja Jyrki Kivimäki

Kustantaja Suomen Atk-kustannus Oy
PL 68
02601 ESPOO
Puhelin (09) 4765 8550
Telekopio (09) 4765 8595
Sähköposti: palvelu@satku.fi
Internet: www.satku.fi

Kansi Frank Chaumont
Timo Ravela (sähköinen versio)

Taitto Jyrki Kivimäki
Reima Flyktman

ISBN 951-762-446-8

Sähköinen laitos Suomen Atk-kustannus Oy
Helsinki 1997

SISÄLLYSLUETTELO

JOHDANTO 1

LUKUOHJE 2
1. WINDOWS NT 4.0 SERVER 5
Käyttökohteet 6
Päivitys Windows NT 3.51:stä 10
Windows NT 4.0 Enterprise Edition 11
Windows NT 5.0 12

2. ASENNUS 15
Ennen asennusta 15
Palvelimen rooli 20
Asennuksessa määriteltävät asetukset 23
Windows NT 4.0 Server CD-ROM 26
Asennusohjelman suoritus 28
CD-ROM 28
Verkko 29
WINNT- ja WINNT32-komennot 32
Palvelimen asentaminen 34
Windows NT 3.51:n päivitys 58
Automaattinen asennus 60
Asennuksen vaiheet 62
Vastaustiedoston luominen 63
Esimerkki vastaustiedostosta 65
Hakemistorakenne ja jaetut resurssit 74
Asennuksen jälkeen 76
Korjauspäivitykset 85
Service Packin asentaminen 87
Windows NT 4.0 Service Pack 2 88
Windows NT 4.0 Service Pack 3 89
HotFixit 90

3. OHJAUSPANEELI 91
Add/Remove Programs 97
Install/Uninstall 97
Windows NT Setup 99
Console 100
Date/Time 101
Devices 103
Dial-up Monitor 108
Internet 109
Licensing 110
Microsoft Mail Postoffice 112
Modems 114
Monitoring Agent 123
Network 124
Identification 126
Services 131
Services 133
Computer Browser 134
NetBIOS Interface 135
RPC Configuration 135
Server 136
SNMP 137
Protocols 138
NWLink IPX/SPX Compatible Transport 139
TCP/IP 140
Adapters 152
Bindings 153
ODBC 154
Ports 154
Printers 157
Add printer 158
General 161
Ports 165
Scheduling 166
Device Settings 168

SCSI Adapters **168**
Devices 169
Drivers 171
Server **175**
Users 176
Shares 177
In Use 178
Replication 179
Alerts 184
Services **185**
System **192**
General 193
Performance 194
Environment 197
Startup/Shutdown 199
Hardware Profiles 203
User Profiles 204
Tape Devices **205**
Devices 205
Drivers 207
Telephony **207**
My Locations 207
Telephony Drivers 208
UPS **210**

4. KÄYTTÖLIITTYMÄ **213**
Suojaukset **213**
Shell 214
Rekisterin asetukset 214
Käyttöliittymän muokkaaminen **215**
Rekisterin asetukset käyttäjän kirjautumisessa 216
Käyttöympäristön asetuksia 217
Käyttöliittymän apuohjelmat 218
Resource Kitin apuohjelmia 219

Desktops 219
Netcons 219
Topdesk 220
Vdesk 220

5. KÄYTTÄJIEN HALLINTA 221
Työryhmän ja toimialueen käyttäjien hallinta 222
Windows NT -työasema 223
Windows NT -toimialue 225
Työryhmä ja toimialue 227
Oletuskäyttäjätunnukset ja -ryhmät 230
Yleiset ja paikalliset ryhmät 233
Erikoiskäyttäjätunnukset ja -ryhmät 243
Toimialueet 244
Palvelinten roolit 244
Primary Domain Controller 246
Backup Domain Controller 247
Stand-Alone Server 248
Luottosuhteet 249
Toimialuemallit 250
Single domain 250
Master domain 251
Master domain -malli laajassa verkossa 258
Multiple master domain 261
Complete Trust 264
Toimialuemallin suunnittelu 267
Käyttäjätietokannan koko 268
User Manager for Domains 269
Uuden käyttäjätunnuksen luominen 270
Ryhmäjäsenyydet 272
Käyttäjäprofiilit 273
Kirjauskomentosarja 281
Kirjautumisajat 290

Kirjautumistyöasemat 293
Käyttäjätunnuksen vanheneminen 294
Käyttäjätunnuksen tyyppi 294
Puhelinyhteys 295
Käyttäjätunnusten kopioiminen 296
Käyttäjätunnuksen asetusten muuttaminen 298
Useiden käyttäjätunnusten asetusten muuttaminen 298
Monien käyttäjätunnusten ryhmäjäsenyyksien hallinta . . 300
Käyttäjätunnusten poistaminen käytöstä 300
Käyttäjätunnusten poistaminen 301
Käyttäjätunnusten nimeäminen uudelleen 302
Paikallisten ryhmien hallinta 303
Yleisten ryhmien hallinta 308
Ryhmään kuuluvien käyttäjien etsiminen 310
Käytännöt ja niiden hallinta 311
Tilikäytäntö 311
Käyttöoikeuskäytäntö 314
Valvontakäytäntö 320
Toimialueen valitseminen 322
Luottosuhteet 323
Luottamisen salliminen toimialueeseen 323
Luotettujen toimialueiden määrittäminen 325
Käyttäjätunnusten hallinta NET-komentojen avulla 329
NET ACCOUNTS 329
NET GROUP 331
NET LOCALGROUP 334
NET USER 336
Käyttäjätunnusten luominen komentojonolla 339

Apuohjelmia käyttäjien hallintaan 343
DUMPACL 343
ADDUSERS 345
GETSID 347
GLOBAL 347
GRPCPY 349
IFMEMBER 351
LOCAL 352
SHOWGRPS 353
SHOWMBRS 353
SRVCHECK 354
USRSTAT 355
USRTOGRP 356
Käyttäjäprofiilit 357
Profiilin rakenne 358
Käyttäjäprofiilien hallinta 360
Palvelimella sijaitseva profiili 362
Pakollinen profiili 363
Palvelimella sijaitsevien profiilien ylläpito 364
Default User 368
Default User palvelimella 368
All Users 370
%USERPROFILE%-ympäristömuuttuja 370
%SYSTEMROOT%-ympäristömuuttuja 373
%COMPUTERNAME%-ympäristömuuttuja 374
Profiilin poistaminen 374
Ohjauspaneeli 374
System Policy Editor 375
Rekisteri 375
DELPROF 376
System Policy Editor 377
Järjestelmäkäytäntöjen periaate 379
Käyttäjien, ryhmien ja tietokoneiden asetusten muuttaminen 381
Toimintatilat ja mallitiedostot 382
Käyttäjän asetukset 387

Control Panel 387
Desktop 388
Shell 389
System 392
Windows NT Shell 395
Windows NT System 402
Tietokoneen asetukset 403
Network 403
System 404
Windows NT Network 405
Windows NT Printers 406
Windows NT Remote Access 407
Windows NT Shell 408
Windows NT System 411
Windows NT User Profiles 413
Paikallisen rekisterin käsittely 414
NTConfig.pol-järjestelmäkäytäntötiedosto 415
Erilliset järjestelmäkäytäntötiedostot 419

6. PALVELIMEN VALVONTATYÖKALUT 421
Palvelimen ja työaseman valvontatyökalujen erot 421
Palvelimen valvontatyökalujen asentaminen työasemaan 424
Administrative Wizards 426
Valvontatyökalut 427

7. VERKKOPALVELUT 431
Palvelimen palvelut 431
Palveluiden lisääminen ja poistaminen 431
Computer Browser 435
NetBIOS Interface 436
RPC Configuration 436
Server 437
NetLogon 443
Browser 450

Vaalit 456
Selauspalvelu reititinverkossa 458
Selauspalvelun konfigurointi 460
Piilotettu tietokone 463
Browser Monitor 463
Browstat 464
Aikakatkaisu 465
Directory Replication 466
Server Manager 469
Toimialueen valitseminen 471
Palvelimen ominaisuudet 473
Jaetut hakemistot 474
Palvelut 475
Viestien lähettäminen 476
Palvelimen roolin muuttaminen 477
Käyttäjätietokannan synkronointi 479
NT-koneen lisääminen toimialueelle 481
NT-koneen poistaminen toimialueelta 484
NT-koneen nimen muuttaminen 484
Toimialueen nimen muuttaminen 485
Palvelimien hallinta NET-komentojen avulla 486
NET ACCOUNTS 486
NET COMPUTER 486
NET CONFIG SERVER 487
NET CONFIG WORKSTATION 488
NET CONTINUE 489
NET FILE 490
NET NAME 491
NET PAUSE 492
NET PRINT 493
NET SEND 494
NET SESSION 495
NET SHARE 496
NET START 498
NET STATISTICS 499
NET STOP 500
NET TIME 501

NET USE 502
NET VIEW 504
Palvelimen hallinta WWW-selaimella 505
Verkkoasemat 509
Kansion jakaminen 509
Kansion jaon lopettaminen 512
Kansiohierarkia 512
Verkkokirjoittimet 515
Kirjoitinohjaimet 515
Verkkokirjoittimen jakaminen 517
Kirjoitinvaranto 519
Kirjoittimien ajastaminen 520
Verkkoon liitetyn kirjoittimen jakaminen 523
Tulostuksen uudelleenohjaaminen 525
Kirjoitinpalvelin 526
Forms 527
Ports 528
Advanced 528
Rekisterin asetukset 529
Tulostusjonot 529
Tulostusilmoitukset 530
Tapahtumaloki 531
Äänimerkki 531
Selauksen esto 532
Network Client Administrator 532
Dial-up Networking 535
Käyttöönotto 537
Rekisterin asetukset 540
Valvonta 542
Dial-up Monitor 542
Remote Access Admin 543
RASLIST 544
RASUSERS 545
Remote Access Manager 545
Apuohjelmia palvelimien hallintaan 545
DIRUSE 546
Domain Monitor 546

FREEDISK 548
INSTSRV 548
NETSVC 549
NLMON 550
NLTEST 551
PERMS 552
Remote Console 553
Remote Command Service 555
Remote Kill 557
RMTSHARE 559
ROBOCOPY 560
SC 561
SCLIST 562
ShareUI 563
Shutdown 564
Shutgui 565
SrvCheck 565
SrvInfo 566
SRVINSTW 567
TIMESERV 567
NetWare Compatible Gateway 569
Yhdyskäytävän periaate 569
Käyttöönotto 570
Asetukset 571
Prosessien välinen kommunikointi 573
Named Pipes ja Mailslots 573
NetBIOS 575
Windows Sockets 576
Etäproseduurikutsut 576
Network Dynamic Data Exchange 577
Server Message Blocks 579
Distributed Component Object Model 580
DCOM:in etuja 581
DCOM:in konfigurointi 581

8. TCP/IP 585
IP-protokolla 586
ARP 586
IP-osoite 587
Isäntätunnus 587
Aliverkko 588
IP-osoiteasetukset Windows NT:ssä 589
Reititys 590
Reititystaulu 591
Oletusyhdyskäytävä 593
Staattinen reititys 593
Route-komento 594
Dynaaminen reititys 596
Moniprotokollareititys 597
Routing Information Protocol (RIP) for TCP/IP 597
DHCP Relay Agent 600
Reitittäminen useiden loogisten aliverkkojen välillä 601
Päällekkäisten IP-osoitteiden havaitseminen 602
Moniosoitteisuus 602
Classless Interdomain Routing 605
IP Multicasting 605
Internet Control Message Protocol 606
Reititystaulujen ylläpito 606
Ongelmanratkaisu ICMP:n avulla 607
Vuonohjauksen säätely ICMP:n avulla 608
Internet Group Management Protocol 609
IP/ARP-laajennukset ja multicasting 610
IP-multicasting ja Windows Sockets -ohjelmat 611
Transmission Control Protocol 611
TCP:n vastaanottoikkunan koko 611
Viivästetyt kuittaukset 612
PMTU-havaitseminen 613
Kuolleen yhdyskäytävän havaitseminen 615
Uudelleenlähetys 617
TCP:n keepalive-viestit 617
Ylikuormituksen välttäminen 618
Silly Window Syndrome 619

Nagle-algoritmi 619
TCP/IP:n tietoturvasuotimet 620
NetBIOS TCP/IP:n päällä 621
Suorituskyky 621
User Datagram Protocol 622
UDP ja nimiselvitys 623
UDP ja mailslot-viestit 623
Transport Driver Interface 623
Verkkosovellusrajapinnat 624
Windows Sockets -rajapinta 625
Nimi- ja osoiteselvitys 625
Backlog-parametri 626
NetBIOS-rajapinta 627
NetBIOS-nimet ja nimiselvitys 628
NetBIOS Scope 631
NetBT-yhteydet 633
NetBT-tietosähkepalvelut 634
NetBIOS-nimien rekisteröinti ja selvitys 635
Solmutyyppi 636
Nimiselvitys usean verkkokortin tapauksessa 639
Windows NT:n Workstation- ja Server-palvelut 640
Yhteyksien muodostaminen verkkoresursseihin 641
WINS 642
Toimintaperiaate 642
WINS-palvelimen käyttöönotto 644
WINS-palvelimen hallinta 645
WINS-palvelinten roolit 648
WINS-palvelun käsittelemät nimet 655
Pysyvät nimien määrittelyt 655
Unique 656
Domain Name 657
Internet Group 658
WINS-tietokannan varmistaminen 659
WINS-tietokannan tiivistäminen 660

Domain Name System 662
DNS-nimipalvelu 663
Verkkoalueet ja niiden osat 665
DNS ja internet 666
Koneennimet 667
Vyöhykkeet 668
Nimipalvelimet 669
Välimuistipalvelimet 672
Nimiselvitys 672
DNS:n asetukset 674
DB-tiedostot 674
Resurssitietueet 675
Resurssitietuetyypit 676
Boot 678
CACHE-tiedosto 678
Käänteisselvitystiedosto 679
Windows NT 4.0 DNS-palvelin 679
Domain Name Service Manager 681
DNS-verkkoalueiden ja vyöhykkeiden lisääminen 681
Vyöhykkeen ja vyöhyketiedoston nimi 683
Välittäjien konfigurointi 685
Tietueiden lisääminen 686
SOA-asetusten muuttaminen 687
Ilmoituslista 687
Käänteisselvitys 688
DNS:n ja WINS:n integrointi 689
Isäntätiedostot 691
DHCP 698
Osoitesarjan luominen ja jakaminen 701
Osoitesarjan asetukset 703
Osoitteiden käyttö 706
Osoitteen varaaminen 707
Tietokannan varmistaminen 708
DHCP:n käyttöönotto työasemassa 708
TCP/IP-apuohjelmia 709
DNSSTAT 709
DHCPCMD 710

WINSCHK 710
WINSCL 710

9. INTERNET-PALVELUT 711
WWW-tekniikka 712
Hypertext Markup Language (HTML) 712
Hypertext Transfer Protocol (HTTP) 712
Uniform Resource Locator (URL) 713
HTTP-linkkiprosessi 715
HTTP-viestit 717
S-HTTP (Secure HTTP) 718
HTTP-NG (Next Generation) 718
Internet Information Server 719
Käyttöönotto 719
IIS:n asentaminen 721
Internet Service Manager 728
WWW-palvelimen asetukset 730
Service 730
Directories 733
Logging 734
Advanced 735
Gopher-palvelimen asetukset 736
Gopher Service 737
Gopher Directories 738
Logging 739
Advanced 739
FTP-palvelimen asetukset 739
Service 740
Messages 741
Directories 742
Logging 743
Advanced 743
Käyttäjätunnukset 743
IUSR_palvelin 744
Anonyymi käyttäjätunnus 749
Käyttäjätunnuksen vaatiminen kirjauduttaessa 752
Kirjautumismekanismi 756
Kirjautumisasetukset 756

Paikallinen kirjautumisoikeus . . . 758
Internet ja Intranet . . . 759
Oikeuksien tarkistaminen intranetissa . . . 760
Oikeuksien tarkistaminen Internetissä . . . 760
Hakemistot . . . 761
Hakemistorakenne . . . 761
Hakemiston lisääminen . . . 763
Hakemiston konfigurointi . . . 769
Hakemiston käyttöoikeudet . . . 770
Oletussivut . . . 772
Hakemistoselaus . . . 773
Virtuaalihakemistot . . . 775
Virtuaalipalvelimet . . . 780
Osoitteiden salliminen ja estäminen . . . 785
Verkkokäytön rajoittaminen . . . 787
HTTP-palvelun laskurit . . . 787
Internet Information Serverin optimointi . . . 793
Secure Sockets Layer . . . 793
Avainparin luominen . . . 795
Sertifikaatin pyytäminen . . . 798
Palvelimen sertifiointi . . . 798
SSL:n aktivointi . . . 799
Microsoft Index Server . . . 799
Käyttöönotto . . . 800
Index Server Administration . . . 801
Kysely . . . 802
Indeksointi . . . 805
Paikallisten hakemistojen indeksointi . . . 805
Etähakemistojen indeksointi . . . 805
Hakemistoihin viittaaminen UNC-nimillä . . . 806
Hakemistoihin viittaaminen levyasematunnuksella . . . 806
Virtuaalipalvelinten hakemistojen indeksointi . . . 806
Indeksoinnin estäminen . . . 807
HTML-tiedostot . . . 808
Windows-verkon etätiedostot . . . 808
Paikalliset NTFS-hakemistot . . . 808
Paikalliset FAT-hakemistot . . . 808
Microsoft Proxy Server . . . 809
Ominaisuudet . . . 809
Toimintaperiaate . . . 811

Ennen asennusta 812
Asentaminen 816
Web Proxy Servicen konfigurointi 819
Service 820
Permissions 821
Caching 822
Logging 823
Filters 824
WinSock Proxy Servicen konfigurointi 825
Service 827
Protocols 827
Permissions 829
Logging 830
Filters 830
Asiakasohjelmien konfigurointi 831
Palvelinlaajennukset 832
Common Gateway Interface 834
Internet Server API 836
Microsoft Visual Basic Scripting Edition 837
ActiveX 838
Active Server Pages 839
IIS ja DCOM 840
Microsoft Transaction Server 840
Java ja JavaScript 841
Open Database Connectivity 842
Microsoft FrontPage 843

10. REKISTERI 845
Rekisterin suojaukset 845
Apuohjelmia rekisterin käsittelyyn 852

11. TIETOTURVALLISUUS 855
Tietoturvallisuuden suunnittelu ja toteuttaminen 857
Suunnittelun lähtökohdat 857
Tiedonhallinta ja valvonta 860
Käyttöoikeudet 861

Pääkäyttäjät tai verkkovastuuhenkilöt 863
Käyttäjien koulutus 866
Katastrofista toipuminen 868
Tietoturvaohje 869
Turvastandardeja 870
Lisätietoa tietoturvallisuudesta 873
Windows NT:n suojausjärjestelmä 877
Ydin 880
Objektit 881
Suojausalijärjestelmä 882
Kirjautuminen 883
Käyttöoikeusluettelot 886
Windows NT:n suojausmenetelmiä 888
Valvontatyökalujen käytön edellytykset 893
Kirjautumisohjeet ja menettelytavat 895
ScanNT 897
Passprop 898
Passfilt 899
Käyttäjätunnukset ja -ryhmät 901
Guest 904
Everyone 906
Hakemistot ja tiedostojärjestelmät 907
Palvelimen ja työaseman käyttöoikeudet 908
NT-koneen piilottaminen 910
Resurssin piilottaminen 911
LogonPrompt 912
Shutdown 912
Automaattinen kirjautuminen 914
NT-koneen työaseman lukitseminen 916
Event Viewerin suojaaminen 917
Kirjoitinohjainten asentamisen rajoittaminen 917
Schedule-palvelun suojaaminen 918
Rekisterin suojaaminen etäkäytöltä 919
Käyttöoikeudet 921
Kansion käyttöoikeudet 921
Tiedostojen käyttöoikeudet 925
Jaetun kansion käyttöoikeudet 928

Jaetun kansion käyttöoikeudet NTFS-levyllä 932
Oletussuojaukset 937
Käyttäjien hallintatyökalujen suojaukset 945
Rekisterin suojaukset 945
Käynnistystiedostojen suojaukset 945
Järjestelmätiedostojen suojaukset 947
Cacls 948
DumpACL 949
Profiilien suojaaminen 949
Roskakori (Recycle Bin) 952
Kirjoittimien suojaaminen 953
Käyttöoikeudet 953
Valvominen 954
Omistus 954
System Policy Editor 955
C2 Configuration Manager 959
File Systems 960
OS Configuration 961
OS/2 Subsystem 962
Posix Subsystem 962
Security Log 962
Halt on Audit Failure 963
Display Logon Message 964
Last Username Display 965
Shutdown Button 966
Password Length 967
Guest Account 968
Networking 969
Drive Letters & Printers 969
Removable Media Drives 969
Registry Security 971
File System Security 972
Other Security Items 973
Suojaustyökaluja 974
Net Watch 976
Process Viewer 977
Pmon 978

Tlist ja Kill 978
Remote Kill 981
Porttien tutkijat 983
Puhelinyhteyksien tutkijat 984
Tapahtumalokien analysointiohjelmat 985
Rekisterien analysointiohjelmat 987
Käyttöoikeusluettelojen analysointiohjelmat 987
Protokolla-analysaattorit 988

Salausmenetelmät 989
Yksisuuntaiset funktiot ja salaovet 991
Sifferit ja Hash-algoritmit 991
Data Encryption Standard (DES) 992
IDEA 993
SAFER 993
Blowfish 993
Skipjack 994
RC-algoritmit 994
Hash-algoritmi 995
Microsoft CryptoAPI 996
Turvallinen tiedonsiirto 997
Microsoft Internet Security Framework 998
Wallet 1000
Personal Information Exchange 1001
Authenticode 1001
Secure Sockets Layer 1001
Secure Hypertext Transfer Protocol 1002
Personal Communications Technology 1002
Secure Electronic Transaction 1002
Secure Sockets Layer 1003
SSL:n käyttö 1004
Point-to-Point Tunneling Protocol 1004
File Transfer Protocol 1006
Domain Name System 1007
RPC-hyökkäys 1008
Out of Band-hyökkäys 1008
SYN-hyökkäys 1008

Etäkäyttäjät 1010
Intranet ja internet 1011
Fyysinen eristäminen 1011
Erilliset protokollat 1013
Internet-palvelimen peilaus 1015
Erillinen reititin 1016
Windows NT -reititys 1018
Vapaa pääsy internetiin 1020
Palomuurit 1021
Internet-palvelimen suojaaminen 1023
Kioski-työaseman suojaaminen 1024
Sähköposti 1028
Virustorjunta 1029
Tiedostojen kopiointi Internetistä 1031

12. JÄRJESTELMÄN KÄYTTÖÖNOTTO JA YLLÄPITO 1033
Käyttöönotto 1033
Suunnittelu 1033
Testaus 1036
Standardointi 1040
Käyttöönotto 1041
Jälkihoito 1042
Windows NT 5.0 1044
Ylläpito 1045
Levytilan hallinta 1046
Varmuuskopiointi 1047
Varmuuskopiointi komentojonojen avulla 1047
Varmuuskopioinnin ajastaminen 1049
SQL Serverin varmuuskopioiminen 1053
Avointen tiedostojen varmistaminen 1054
Järjestelmän palauttaminen nauhalta 1054
Levyjen hallinta 1055
Stripe Set with Parity 1055
Mirroring 1056
Tapahtumien valvonta 1058
Suojauslokin käyttö järjestelmän valvonnassa 1060
LOGEVENT 1063

Käytännön vinkkejä 1064
The credentials supplied conflict with an existing set of credentials 1064
AutoExNT 1065
Käyttäjien avoimet tiedostot 1066
Järjestelmäkäytäntö lukinnut pääkäyttäjän 1066
Sivutustiedoston poistaminen 1067
Dr Watsonin deaktivointi 1068
Viestit 1068
Hälytykset 1069
WinMSDP 1071
Drivers 1071
Levytilan ilmoitus 1072
Palvelimen alasajo 1073
NTFSDOS 1074
NTFS-buuttidisketti 1074
Käynnistysongelmat 1075
Blue Screen of Death 1076
Windows NT 4.0 Server Resource Kit 1077
Muita työkaluja 1078
Optimointi 1079
Palvelinlaitteisto 1081
Käyttötarkoitus 1081
Merkkivalmistajan laite vai itse rakennettu 1082
Vikasietoisuus 1085
Prosessori 1085
Keskusmuisti 1087
Väylä 1088
Virtalähde 1089
Näyttö 1089
Laitekotelo 1089
Levyjärjestelmä 1089
Varmistuslaitteet 1092
CD-ROM 1092
Verkkokortti 1092
Modeemi 1093
UPS 1094

Windows NT Server 1094
Muistin säätäminen 1095
Prosessorin tehokkuuden säätäminen 1102
Levyjärjestelmän tehokkuuden säätäminen 1105
Palvelinlaitteistoja 1108
Compaq ProLiant 6000 1108
Digital Prioris 6000 ZX 1109
HP NetServer LX Pro 1110
IBM Server 704 1111
NCR 4300 1112
Tandem S1000 1113
Klusterit 1114
Käsitteitä 1114
Ominaisuuksia 1115
NCR LifeKeeper 1118
Windows NT Cluster Server 1119
Tandem ServerNet SAN 1120

JOHDANTO

Tervetuloa **Windows NT 4.0 Tehokäyttäjän Oppaan Osan 2** pariin. Kirjan tarkoitus on johdattaa sinut tehokkaasti **Windows NT 4.0** -käyttöjärjestelmän palvelinversion (Server) pariin. Työasemaversiota käsitellään **Osassa 1**.

Kirjassa on lukuisia käytännön esimerkkejä, joita olen laatinut mm. vetämilläni kursseilla saamieni palautteiden mukaan. Toivon, että olen osannut tuoda kokemukseni esille myös tässäkin kirjassa! Palautteesi voit antaa lähettämällä kustantajalle kirjan lopusta löytyvän palautelomakkeen.

Kirja on kirjoitettu **ICL ErgoProlla** (Pentium Pro 150 MHz) ja **HP Vectra XU 6/200** (2 x Pentium Pro 200 MHz). Palvelimia on ollut käytössä nelisenkymmentä erilaista, alkaen **Tandem S1000** (4 x Pentium Pro 200 MHz) ja **NCR 4300** (4 x Pentium Pro 150 MHz) päättyen muutaman **Compaq ProLiant**in ja **Hewlett-Packard LX**:n kautta Opti-emolevyllä varustettuun **AMD 486/66**:een. Nestemäisestä puolesta voin mainita kirjoitustyössä kuluneet lähes sata **Battery**-tölkkiä.

Haluan kiittää läheisiäni saamastani supportista:

- **Helena**
- **Lauri**

sekä seuraavia instansseja:

- **Jukka Issakainen**, Nokia Telecommunications Oy, käsikirjoituksen kommenteista (kirjassa mahdollisesti esiintyvät mokat ovat kirjoittajan)
- **Incos Oy** erinomaisesta laitteistosupportista (*aamuin illoin*)
- **Fabulous Thunderbirds**in tuotantoa inspiraation lähteenä.

Espoo 17.7.97
Jyrki Kivimäki

LUKUOHJE

Tämä opas jakaantuu 12:een lukuun. Voit edetä opasta aivan vapaasti omassa tahdissasi tai loikata suoraan kiinnostavaan aiheeseen:

1. luku käsittelee lyhyesti Windows NT 4.0 Serveriä (myös Enterprise Edition) ja Windows NT 5.0:aa

2. luku keskittyy Windows NT Serverin **asentamiseen**

3. luku käy läpi Windows NT Serverin **Ohjauspaneelin** asetukset

4. luku esittelee **käyttöliittymän** hallintamahdollisuuksia

5. luku käsittelee **käyttäjienhallinnan**

6. luku esittelee lyhyesti Windows NT Serverin mukana tulevat **valvontaohjelmat**

7. luku käsittelee verkkopalveluita

8. luku käsittelee **TCP/IP-protokollaa** Windows NT:ssä

9. luku käsittelee Windows NT:n Internet-palveluita

10. luku käsittelee lyhyesti Windows NT Serverin rekisteriä

11. luku paneutuu **tietoturvallisuuteen**

12. luku tarkastelee Windows NT Server -järjestelmän **ylläpitoa**.

Kirjassa käytettyjä termejä:

- **NT-kone** on mikä tahansa Windows NT-mikro, versiosta riippumatta (3.1-4.0)

- **NT-työasema** on mikä tahansa Windows NT-työasema, versiosta riippumatta (3.1-4.0). Tarvittaessa on mainittu erikseen Windows NT 4.0-työasema

- **NT-palvelin** on mikä tahansa Windows NT-palvelin, versiosta riippumatta (3.1-4.0). Tarvittaessa on mainittu erikseen Windows NT 4.0-palvelin

- **Toimialue** (*Domain*) käsittää keskitetyn ja yhtenä kokonaisuutena hallitun käyttäjätunnusten, käyttäjäryhmien ja NT-konetunnusten joukon

- **PDC** tarkoittaa toimialueen (*Domain*) **ensisijaista ohjauskonetta** (*Primary Domain Controller*, myös termiä **pääpalvelin** käytetään joissakin suomennoksissa)

- **BDC** tarkoittaa toimialueen varaohjauskonetta (*Backup Domain Controller*, myös termiä **varapalvelin** käytetään joissakin suomennoksissa)

- **Ohjauskone** (*Domain Controller*) on joko PDC tai BDC. Tarvittaessa on selitetty, kumpi on kyseessä

- **Stand-alone Server** on erillinen palvelin, joka ei ole kuulu toimialueen keskitetyn hallinnan piiriin (myös nimityksiä **Member Server** ja harhaanjohtavaa **Server** - suomennoksissa ehkäpä vain palvelin - käytetään)

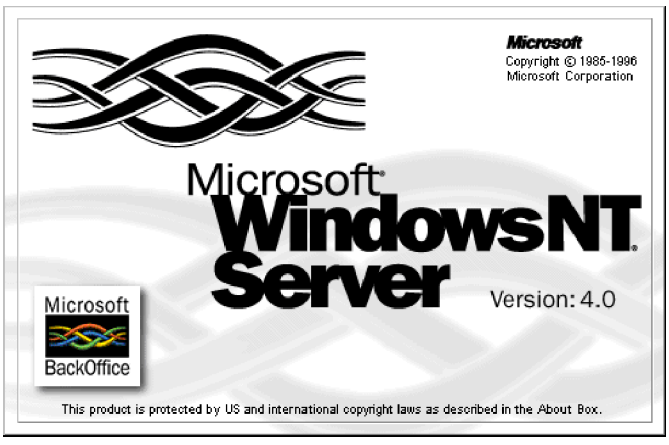
- **Pääkäyttäjä** viittaa paitsi verkkovastaavaan tai PC-tukihenkilöön, myös Windows NT:n **Administrator** -käyttäjätunnukseen tai **Administrators**-ryhmän jäseneen. Kyseessä on käyttäjä, jolla on täydet valtuudet hallinta NT-ympäristöä.

1. WINDOWS NT 4.0 SERVER

Windows NT 4.0 julkistettiin heinäkuussa 1996 ja se tarjoaa paljon uusia ominaisuuksia. Kirjoittajan mielestä seuraavat viisi piirrettä ovat keskeisiä muutoksia:

- **Arkkitehtuurimuutokset, tähtäimessä tehostunut suorituskyky**
- **Windows 95-näköisyys**
- **Järjestelmänhallinnan kehittynyt tuki**, Tehtävänhallinta (Task Manager)
- **Käyttäjän ympäristön kehittynyt hallinta** - profiilit, **Järjestelmäkäytäntöjen editori** (*System profile Editor*), oletuskäyttäjän (*Default User*) ja kaikkien käyttäjien (*All Users*) yhteiset asetukset
- **Internet/Intranet-tuki** sekä työasemassa että palvelimessa; mukana tulevat **WWW-palvelimet ja -selain**, palvelimessa myös **DNS** (*Domain Naming System*).

Kaksi viimeistä muutosta liittyy läheisesti Windows NT:n käyttöön verkkoympäristössä, ja niihin (sekä moniin muihin palvelimeen liittyviin asioihin) tutustutaan tässä kirjassa.



Käyttökohteet

Missä tilanteissa pitäisi käyttää Windows NT-palvelinta?

Kirjoittajan oma suosikkilista asioista, joiden perusteella voit harkita, tarvitsetko ylipäätään palvelimen:

- Lähiverkkoa ei ole ollenkaan käytössä
- Lähiverkko on pieni (alle 10 kymmenen työasemaa)
- Käyttäjien sovellukset on asennettu mikroihin paikallisesti
- Käyttäjien työtiedostot tallennetaan mikroihin paikallisesti, ja niiden varmuuskopiointi on kunnossa
- Ei tarvita erillisiä käyttäjätunnuksia
- Ei tarvita keskitettyä käyttäjien hallintaa
- Ei tarvita kehittynyttä tietoturvallisuutta
- Tietoliikenneyhteyksissä (sähköposti, internet) tukeututaan modeemiyhteyksiin
- Ja lopuksi: nykyinen ympäristö palvelee käyttötarkoitustaan riittävästi.

Mitä useammassa argumentissa olet samaa mieltä, sitä todennäköisempää on, että et tarvitse palvelinta. *Jos* tarvitset, seuraava kysymys onkin, tarvitsetko Windows NT-palvelimen, OS/2-, Novell NetWare-palvelimen vai ehkä jonkin Unix-palvelimen.

Tässä kirjassa käsitellään Windows NT-palvelimen eri käyttökohteita, joten saatat saada hyviä vinkkejä siitä, missä eri tilanteissä ehkä voisit Windows NT-palvelinta soveltaa.

Vaikka käytettävissä ei olisikaan omaa lähiverkkoa, Windows NT -palvelinta voi silti seuraaviin tehtäviin:

- Etäkäyttöpalvelimena (*Remote Access Server*), jolloin päästään esimerkiksi modeemiyhteydellä palvelimen resursseihin
- Etäkäyttöpalvelimena internetiin - tällöin päästään esimerkiksi modeemiyhteydellä palvelimen kautta internet-yhteyteen
- Internet-palvelimena (WWW-, Gopher- ja FTP-palvelimet tulevat NT-palvelimen mukana).

Näitä ominaisuuksia voi tarjota myös Windows NT -työasema, mutta siinä etäkäyttöpalvelu on rajoitettu yhdelle samanaikaiselle käyttäjälle. Lisäksi NT-työasema ei tue kuin kahta prosessoria, eli tarvittaessa CPU-suorituskyky NT-palvelin on selkeä vaihtoehto.

Tämän johtuu siitä, että Windows NT Workstation ja Windows NT Server on tarkoitettu eri käyttöä varten:

- Windows NT Workstation on tarkoitettu työasemakäyttäjille, jotka haluavat tehon lisäksi skaalattavuutta, vikasietoisuutta sekä NT:n suojausominaisuuksia.
- Windows NT Server on palvelinohjelmisto sovelluspalvelimeksi, tiedosto- ja tulostuspalvelimeksi sekä etäkäyttöpalvelimeksi.

Jos haluat käyttää Microsoft-ympäristön palvelinsovelluksia (Internet Information Server, SQL Server, SNA Server, Transaction Server, Proxy Server, Exchange, Systems Management Server jne) on Windows NT -palvelin ainoa vaihtoehto.

Haluttaessa keskitetty käyttäjien ja resurssien hallinta pitää tukeutua Windows NT -palvelimeen. Tällöin voidaan hyödyntää toimialueen (*domain*) keskitetyn resurssienhallinnan etuja.

Seuraavat toiminnot tulevat vain Windows NT -palvelimen mukana -työasemaversioon ne eivät kuulu:

- **Dynamic Host Configuration Protocol** (DHCP) -palvelinpalvelu (sekä työasema- että palvelinversio sisältävät DHCP-protokollan asiakkaan)
- **Windows Internet Naming Service-** (WINS) ja **Domain Naming System-** (DNS) nimipalvelut
- Keskitetty käyttäjähallinta
- Kiintolevyjärjestelmän vikasietoisuusominaisuudet (peilaus jne)
- Etäkäyttöpalvelimen (Remote Access Server) 255 samanaikaista käyttäjää (työasemassa yksi)
- Yhdyskäytävä NetWare-palvelimeen (Gateway Services for NetWare, GSNW)
- Macintosh-palvelut: tiedosto- ja kirjoitinpalvelut Macintosh-käyttäjille, AppleTalk-kirjoittimet sekä Macintosh- että Windows-käyttäjille
- Logon scriptit
- Käyttäjätunnusten lukitseminen
- Verkkotyöasemien asennustuki (Network Client Administrator)
- Toimialueen hallintavälineet (Server Manager, User Manager for Domains)
- RPL-tuki levyttömille työasemille
- Lisenssipalvelu.

Toiminto	Windows NT Server	Windows NT Workstation
Tavoite	Palvelinpalvelut mahdollisimman tehokkaat - kaikki käytettävissä olevat CPU/muistiresurssit palvelevat resurssien jakoa	Työasemapalvelut mahdollisimman tehokkaat työaseman paikalliselle käyttäjälle
SMP	Tukee neljää prosessoria	Tukee kahta prosessoria
Muisti	Minimi 16 Mt RAM Suositus > 32 Mt RAM	Minimi 12 Mt RAM Suositus > 16 Mt RAM
Levytila	Minimi 160 Mt	Minimi 110 Mt
Asiakkaiden verkkoyhteyksien lkm	Rajoittamaton	10
Apple MacIntosh-tuki	On	Ei
Vikasietoisen levyjärjestelmän tuki	RAID 1 ja RAID 5	Ei
Toimialuetuki	On	Ei
Etäkäyttöpalvelin	256 samanaikaista käyttäjää	1 käyttäjä
Monistuspalvelu (Replikointi)	Vienti/tuontipalvelu	Tuontipalvelu
Hallintavälineet	NT-palvelimien ja NT- työasemien hallinta	Vain paikallisen NT-työaseman, mutta osa työkaluista tukee NT-palvelimien ja -työasemien hallintaa
BackOffice -palvelinalusta	On	Ei
HTTP-, Gopher-, FTP-palvelin	Rajoittamaton	Rajoitettu
DNS-, DHCP- ja WINS-palvelin	On	Ei
FrontPage-editori	On	Ei

Päivitys Windows NT 3.51:stä

Kannattaako päivittää Windows NT 3.51 -ympäristö Windows NT 4.0:aan?

Päivityksen hyödyllisyyttä on syytä harkita, jos:

- Palvelimet toimivat moitteettomasti (ja niihin on asennettu uusin korjauspäivitys, mikä kesäkuussa 1997 oli edelleen Service Pack **5**)
- Et tarvitse Windows NT 4.0 Serverin uusia ominaisuuksia (IIS ja Active Server Pages, DCOM, DNS, DFS jne)
- Käytettävät palvelinsovellukset eivät tarvitse (saati tue) Windows NT 4.0:ää.

On hyvä muistaa, että jos yllättäen tulee esiin tarve päivittää palvelimet Windows NT 4.0-versioon, sitä ei *välttämättä* tehdä hetkessä ja uuden ympäristön ominaispiirteiden oppiminen vie oman aikansa!

Windows NT 4.0:n viimeisin korjauspäivitys oli kesäkuussa 1997 Service Pack **3** - ja se tuntuu olevan jo riittävän vakaa.

Työasemien tapauksessa tilanne on ehkä jopa yksinkertaisempi. Windows NT 4.0 -työasemakäyttäjän profiilit toimivat myös Windows NT 3.51 -palvelinympäristössä. Profiilit eivät tosin ole yhteensopivia (eivät myöskään Windows 95 -profiilit),

Windows NT 4.0 Enterprise Edition

Windows NT 4.0 Enteprise Edition on uusin Windows NT Server -paketointi.

Sen keskeiset piirteet ovat:

- **Microsoft Cluster Server** (MSCS) -ohjelmisto (*Wolfpack*, versio 1.0). Klusteri (*ryväs*) on vähintään kahden palvelimen (*node*) muodostama vikasietoinen ympäristö. Jos sovellus kaatuu toisessa palvelimessa, se voidaan käynnistää automaattisesti toisessa palvelimessa. Koska kyseessä on käyttöjärjestelmän ylätason ratkaisu, se on myös laitteistoitsenäinen. MSCS API-rajapinnalla voidaan rakentaa sovelluksia, joiden kuormitus tasataan eri palvelimien välillä. Tällaisista sovelluksista käytetään nimitystä *Shared nothing*

- Tuki kahdeksalle prosessorille (*Symmetric multiprocessing* (SMP)) skaalattavuuden lisäämiseksi

- Sovellukset saavat käyttöönsä uudella muistinhallinnalla **3 GB** keskusmuistia (RAM) (nykyinen rajoitus 2 GB)

- **Microsoft Transaction Server** (MTS) ja **Microsoft Message Queue Server** (MSQS) tuovat luotettavuutta ja skaalautuvuutta tapahtumankäsittelyn ja niiden sanomien hallintaan. MTS:n avulla eri sijaintipaikoissa olevat tietokannat saadaan päivitettyä hajautettujen sovellusten avulla. MSQS varmistaa sanomien perillemenon. Komponettipohjaisuus tukee sovellusympäristön aiempaa helpompaa päivitysmahdollisuutta - esimerkiksi voidaan valita vaihtoehtoiset reitit sanomien välitykseen

- **Microsoft Index Server** tukee tiedon hakemista WWW-palvelimen kautta

- **Distributed Component Object Model** (DCOM) tukee DCOM-sovellusten toimintaa - myös Internetissä.

Minim laitteisto- ja ohjelmistovaatimukset **Windows NT 4.0 Server Enterprise Edition** -palvelimelle ovat:

- Pentium (90 MHz) tai uudempi, tai DEC Alpha
- 64 Mt RAM
- 500 Mt vapaata kiintolevytilaa
- Microsoft SQL Server 6.5 (Microsoft Message Queue Server vaatii)
- VGA tai Super VGA
- CD-ROM-asema
- Hiiri.

Windows NT 5.0

Windows NT 5.0:n ennakkotietojen mukaan keskeisessä asemassa tulevat olemaan:

- S**elkeämpi keskitetty hallinta** - keskitetyt päivitetykset, keskitetyt sovellusten asennukset, keskitetty työasemien hallinnointi, keskitetty järjestelmän lukitseminen jne. PDC ja nykyisenkaltaiset toimialuemallit katoavat. Palvelimia voi vapaasti siirtää toimialueelta toiselle

- **Distributed File System** (DFS) - hajautettu tiedostojärjestelmä, jonka beta Windows NT 4.0:lle löytyy jo nyt Microsoftin WWW-palvelimesta. Idea on se, että kotihakemiston kytkeminen onnistuu vihdoinkin komennolla **NET USE H: \\V1\USERS\JKI**

- **Active Directory** on objektipohjainen hakemistoratkaisu, perustuu CCITT X.500-standardiin ja Lightweight Directory Access Protocol (LDAP)-protokollaan, jossa objektit nimetään esimerkiksi CN=jurgen steinhugel,OU=pctuki,O=fishware, C=fi.- Järjestelmää hallitaan pääasiassa yhdellä sovelluksella, **Microsoft Management Modulella** (MMC) sekä **Internet Explorerilla**

- **Active Server** -tuki Internet/Intranet-sovelluskehitykseen laajenee

- **TCP/IP**:lle tulee **Quality of Service** (QoS)-tuki

- **Universal Serial Bus** (USB)- ja **P1394**-tuki
- **Kytke ja käytä** -tuki tulee vihdoinkin, ja mahdollisesti Windows 9x (*Memphis*) -yhteensopivat laiteohjaimet
- 64-bittinen virtuaalimuistinhallinta (*Very Large Memory*) jää nähtäväksi.

Muuta tervetullutta *saattaa* olla esimerkiksi *Rapid booting* (työaseman käynnistys sekunneissa) ja tosiaikainen multimedia (myös 3D- ääni).

2. ASENNUS

Seuraavaksi käsittelen Windows NT 4.0 Server -version asennusta. Esimerkit pohjautuvat Microsoftin Windows NT 4.0 Server -CD-ROM:ilta suoritettaviin asennuksiin.

Olen pyrkinyt käsittelemään useita mahdollisia asennuksen vaihtoehtoja. Siksi asennusohjeet saattavat sisältää valintoja, joihin et omassa asennuksessasi törmää.

Eräillä laitevalmistajilla (mm. Compaq ja Hewlett-Packard) on omia asennusohjeitaan ja -menetelmiään. Tutustu niihin huolellisesti ennen asentamista!

Laitteistoa on käsitelty myös **luvussa 10**.

Ennen asennusta

Varmista, että asennettavassa mikrossa on riittävä laitteisto:

- **80486/33 MHz tai tehokkaampi Intelin prosessori** (mieluummin **Pentium**; **Pentium Pro** suositeltavin; mitä nopeampi, sen parempi)
- **16 Mt tai enemmän keskusmuistia** (32 Mt suositeltava minimi palvelimessa. Tarvittava muistin määrä riippuu käyttäjämäärästä ja palveluista)
- **CD-ROM-asema** tai verkkoyhteys CD-ROM:iin
- **Vähintään 160 Mt vapaata kiintolevytilaa** (suosittelen käyttämään SCSI-kiintolevyä ja lisäksi varaamaan palvelimella 300 - 500 Mt levyosion NT-järjestelmäosioksi)
- VGA-näyttö
- Hiiri

- HD-levykeasema
- Verkkokortti
- Äänikortti ei ole palvelimessa pakollinen (ISA-väylän äänikorttia en edes suosittele).

tai

- **Windows NT:n tukema RISC-prosessori** (DEC:in **Alpha** suositeltavin; muiden RISC-prosessorien tuki on päättynyt)
- **16 Mt** tai enemmän keskusmuistia
- **CD-ROM-asema** tai verkkoyhteys CD-ROM:iin
- **Vähintään 160 Mt vapaata kiintolevytilaa** (suosittelen käyttämään SCSI-kiintolevyä)
- VGA-näyttö
- Hiiri
- HD-levykeasema
- Verkkokortti.

Huomattavaa:

- CD-ROM-asema voi olla **SCSI** tai **ATAPI**. Lisäksi tarvitset vähintään yhden, mahdollisesti neljä tyhjää HD-levykettä. Yksi tarvitaan korjauslevykettä (**Emergency Repair Disk**) varten

- Jos käytät kaksois- tai useammalla prosessorilla varustettua mikroa, varmista ennen hankintaa järjestelmän toimivuus käyttämässäsi Windows NT-versiossa. Tarkista myös referenssit! (Jos NT ei asennus moniprosessorimikroon, kokeilepa *ROM Shadowing*-toiminnon kytkemistä pois käytöstä)

- Onko kyseessä NT:n päivitys vai uusi asennus: jos kyseessä on uusi asennus, valitse levyn osiointi, tiedostojärjestelmä ja hakemisto, minne NT asennetaan

- NT ei tue **DriveSpace**- tai **DoubleSpace** (eikä muitakaan) levyjen pakkausmenetelmiä. NT:n oma pakkausmenetelmä ei ole yhteensopiva minkään muun pakkausmenetelmän kanssa (jaettaessa hakemistoja palvelimelta NT:n pakkausmenetelmä on kuitenkin käyttäjien kannalta läpinäkyvä)

- NT:n asennusohjelma osaa käyttää **OnTrack Disk Managerilla** osioituja levyjä

- Windows NT 4.0 ei tue HPFS-tiedostojärjestelmää! Jos päivität Windows NT-mikron, jossa on HPFS-levy, Windows NT 4.0:ään, niin muunna CONVERT-komennolla HPFS-levy NTFS-levyksi ennen asennusta!

- Vaikka kyseisessä mikrossa DOS toimisikin, se ei tosiaankaan tarkoita että automaattisesti myös NT toimisi! NT on huomattavasti kriittisempi laitteiston asetuksille kuin DOS (SCSI:n terminointi, keskeytykset (IRQ) jne).

Selvitä myös seuraavat palvelimen **tekniseen kokoonpanoon** liittyvät asiat:

- PCI-väylän asetukset ja tarvittaessa keskeytysten varaaminen ISA-väylän korteille
- Näytönohjain tai ainakin käytetty piirisarja (S3 jne), halutut näytön asetukset (resoluutio, virkistystaajuus)
- SCSI-ohjain - tyyppi tai ainakin käytetty piirisarja, IRQ, I/O-osoite, DMA (jos käytetty)
- Hiiri - tyyppi, liitäntäportti (sarjaportti COM1/COM2 tai tai PS/2)
- Modeemi - ulkoisen modeemin tyyppi ja liitäntäportti (sarjaportti COM1/COM2 tai sisäisen modeemin tyyppi ja IRQ sekä I/O-osoite
- Mahdollinen äänikortti - tyyppi, IRQ, I/O-osoite, DMA (jos käytetty; äänikortti ei ole palvelimessa pakollinen, ja ISA-väylän äänikorttia en edes suosittele)
- Edellisten selvittämisessä apunasi voit käyttää NT:n mukana tulevia **NT Hardware Query Tool**- ja **SCSI Tool**-apuohjelmia. DOS-pohjaiset apuohjelmat, kuten MS-DOS:in **MSD** (Microsoft Diagnostics) eivät välttämättä toimi luotettavasti!
- Laitteiston toimivuus on myös hyvä testata ennen asennusta esimerkiksi laitteistovalmistajan omalla diagnostiikkaohjelmalla (esim. **Compaq Diagnostics**). Testaa **emolevy** (CPU, aritmetiikkaprosessori (*Math coprocessor*), DMA- ja keskeytyskontrolleri, CMOS-kello ja tarvittaessa EISA- ja MCA-väylä ohjaimineen), **muistit** (*RAM*: perusmuisti (*Base Memory*) ja jatkettu muisti (*Extended Memory*)), **näytönohjain** (*Video Adapter*, *Video RAM Mono* ja *VGA-mode*), kiintolevyt ohjaimineen (*Hard Drive*; kannattaa valita *non-destructive*-tyyppinen testi, joka ei tuhoa levyn tietoja (*random-, linear-, butterfly cylinder access*), levykeasemat, CD-ROM (lukutesti ja levyn poisto asemasta, *random-, linear-, butterfly sector access*), sarja- ja rinnakkaisporttitestit
- Kytke ennen NT:n asennusta sarjaporttiin kytketty **UPS** pois

päältä.

SCSI-laitteissa huomattavaa:

- NT:n SCSI- ja CD-ROM-tuki edellyttää **SCSI-väylän pariteetti-tarkistuksen** käyttämistä. Tämä on usein konfiguroitavissa oleva asetus, joten tarkista asetus omassa laitteistossasi. Esimerkiksi **NEC CDR-36**- ja **NEC CDR-37**-asemat **eivät** tue tätä ominaisuutta

- Tarkista, että kaikilla SCSI-väylän laitteilla on oma **ID-tunnus**. Buuttaavan kiintolevyn tulisi olla **ID 0**

- Tarkista SCSI-väylän **terminointi**. Väylän ensimmäisessä ja viimeisessä laitteessa tulee olla terminointi käytössä. Jos samassa väylässä käytät sekä ulkoisia että sisäisiä laitteita, poista terminointi SCSI-ohjaimesta. Jos poistat SCSI-laitteen, tarkista, että SCSI-väylän terminointi on edelleen oikein asetettu
- Jos SCSI-ohjain sisältää kaksi väylää (esim. 50- ja 68-johtimiset tavallisen- ja Wide-SCSI:n), tarkista tällöin erityisen huolellisesti SCSI-väylän **terminointi**

- SCSI-väylän terminointi vaatii oman syöttönsä (*termination power*), joko SCSI-ohjaimelta tai joltakin oheislaitteelta

- Kaapeleiden minimipituus on 30 cm ja maksimipituus 6 m

- Käynnistä ensin ulkoiset SCSI-laitteet ja vasta sitten mikro

- Kaikki SCSI-laitteet eivät ole keskenään yhteensopivia tai yhteensopivia kaikkien SCSI-ohjainten kanssa

- Väärin asennettu SCSI-ohjain, -oheislaite tai -väylä voi johtaa NT:n asennusongelmiin tai tiedostojen korruptoitumiseen.

Verkkokorteissa huomattavaa:

- Käytä mieluimmin tehokkaita PCI-väylän verkkokortteja
- Selvitä verkkokortin tyyppi, keskeytykset (**IRQ**), I/O-osoite, DMA (jos käytetty), liitäntätyyppi (BNC, RJ-45 jne) jne. Windows NT käyttää tunnistettuja oheislaitteita oletusarvoilla
- Eksoottinen verkkokortti saattaa toimia jollakin emulaatiolla, esimerkiksi **NE2000**. Verkkokortissa saavutettu muutaman sadan markan säästö saattaa kuitenkin *myöhemmin* maksaa huomattavasti enemmän
- Windows NT-palvelinta ei voi asentaa ilman verkkotukea. Jos et voi asentaa verkkokorttia, yritä asentaa **MS Loopback Adapter** (löytyy verkkokorttien listasta asennusvaiheessa). Tällöin voit jatkaa asennusta (riippuen palvelimen tyypistä) ja yrittää asentaa Windows NT:n loppuun saakka.

Palvelimen rooli

Asennusohjelmassa tulee ottaa kantaa siihen, mikä tulee olemaan palvelimen rooli verkossa. Palvelimella voi olla kolme roolia eli tyyppiä:

Ensisijainen ohjauskone (Primary Domain Controller, PDC):

- Asennetaan toimialueen ensimmäisenä palvelimena
- Ylläpitää käyttäjätietokantaa ja toimialueen asetuksia
- Käsittelee käyttäjän kirjautumispyynnöt toimialueelle
- Voi toimia tiedosto-, tulostin- tai sovelluspalvelimena
- Lukumäärä on **tasan yksi kappale per toimialue**

Ohjauskone (Backup Domain Controller, BDC) (myös nimityksiä varakone tai varapalvelin käytetään):

- Saa kopion käyttäjätietokannasta
- Toimii varapalvelimena, jos ensisijainen ohjauskone (PDC) ei ole jostain syystä verkossa tai ei kerkiä vastaamaan
- Käsittelee käyttäjän kirjautumispyynnöt toimialueelle
- Voi toimia tiedosto-, tulostin- tai sovelluspalvelimena
- Toimialue ei edellytä yhtään varapalvelinta, mutta oma suositukseni **on vähintään yksi kappale per toimialue**; maksimi lukumäärää ei ole rajoitettu. Jos BDC ei jaa resurssejaan verkkoon, vaikkapa **i486/33** riittävällä muistilla *saattaa* riittää; tilannetta voit toki aina valvoa **Performance Monitorilla**. Ilman Domain Controlleria käyttäjät eivät voi kirjautua toimialueelle!

Palvelin (Stand-Alone Server tai Server):

- Voi toimia tiedosto-, tulostin- tai sovelluspalvelimena
- Ei saa kopiota käyttäjätietokannasta - edellyttää siis omaa paikalliusta käyttäjien hallintaa

Stand-Alone Server-tyyppisen palvelimen liittäminen toimialueelle voidaan tehdä asennuksen yhteydessä tai jättää palvelin liittyneeksi työryhmään. Erot ovat seuraavat:

Palvelin liitetty työryhmään (Workgroup):

- Stand-Alone Server-tyyppinen palvelin toimii kuten työryhmään määritelty NT-työasema. Ei keskitettyä käyttäjien hallintaa - käyttäjät määritellään työasemakohtaisesti palvelimen käyttäjien hallinnalla
- Ei keskitettyä resurssien käyttöoikeuksien hallintaa.

Palvelin liitetty toimialueelle (Domain):

- Stand-Alone Server-tyyppinen palvelin toimii kuten NT-työasema. Voidaan tukeutua toimialueen keskitettyyn käyttäjien hallintaan - esimerkiksi käyttäjien ryhmäjäsenyydet voidaan määritellä

- Resurssien käyttöoikeuksien hallinta voidaan toteuttaa käyttämällä hyväksi toimialueen käyttäjätunnuksia ja -ryhmiä

- Resurssien hallinta voidaan hoitaa esimerkiksi NT-palvelimelta tai toisesta toimialueelle liittyneestä NT-työasemasta.

Missä sitten saatetaan tarvita Stand-Alone Server-tyyppistä palvelinta? Seuraavassa eräitä ehdotuksia:

- Käyttäjät eivät kytkeydy Stand-Alone Server-tyyppisen palvelimen resursseihin NT:n käyttäjätunnuksilla (esimerkiksi kyseessä on välityspalvelin (*proxy*), tietokantapalvelin, anonyymi-FTP- tai WWW-palvelin)

- Halutaan lisäsuojauksia sillä, että tavalliset verkon käyttäjät eivät voi kytkeytyä Stand-Alone Server-tyyppisen palvelimen resursseihin NT:n käyttäjätunnuksilla

- Saadaan lisää suorituskykyä, koska Stand-Alone Server-tyyppinen palvelin ei käsittele toimialueen käyttäjien kirjautumispyyntöjä eikä se myöskään saa toimialueen käyttäjätietokannan kopiota

- Stand-Alone Server on siirrettävissä toiseen toimialueeseen tai työryhmään.

Vaikka saattaakin kuulostaa siltä, että **Stand-Alone Server** on sopiva ratkaisu joihinkin palvelintoimintoihin, muista kuitenkin, että yhden Stand-Alone Serverin ylläpito saattaa pahimmillaan aiheuttaa kaksinkertaisen määrän työtä!

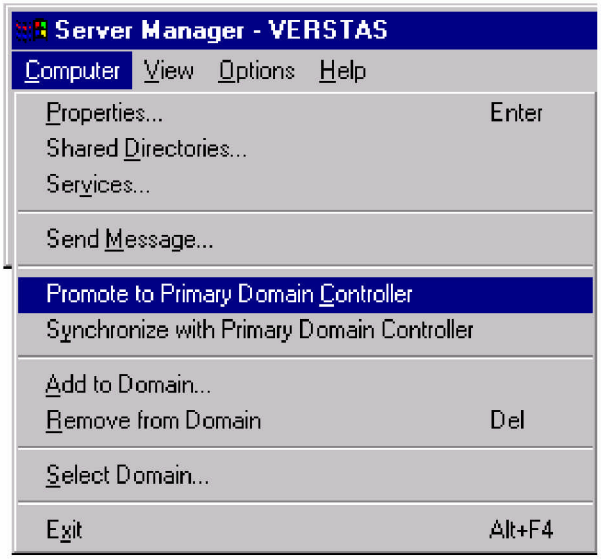
Asennuksessa määriteltävät asetukset

Omasta ympäristöstäsi riippuvat seuraavat kokoonpanoon liittyvät asiat:

- Aika ja aikavyöhyke
- Käytetyt maakohtaiset asetukset (kieli, näppäimistö jne)
- Protokollat asetuksineen
- Palvelimen **nimi** ja **rooli** verkossa. Nimi ei saa olla minkään toimialueen tai työryhmän nimi. Suunnittele nimeämisstandardit esim. osaston, maantieteellisen sijainnin tms mukaan. Varaudu palvelmien lisäämiseen ja siirtämiseen paikasta toiseen. Älä käytä nimessä merkkejä ¤, , ¦, §, ¶, *, ?
- Asennettaessa reititinverkossa NT-työasemaa tai -palvelinta olemassa olevalle toimialueelle on syytä myös selvittää toimialueen **ensisijaisen ohjauskoneen** (PDC, Primary Domain Controller) **IP-osoite** sekä luotava kelvollinen **LMHOSTS**-tiedosto. Muuten yhteyttä ei ohjauskoneeseen saada, ja ainakin toimialueen **varapalvelimen** (BDC, Backup Domain Controller) asennus tyssää siihen
- **Primary Domain Controllerin** (PDC) ja **Stand-Alone Serverin** tapauksessa määritellään Administrator-käyttäjätunnuksen salasana
- Jos palvelin liittyy olemassaolevaan **työryhmään** tai **toimialueeseen**, myös tämän nimi on tiedettävä
- Kirjoittimen tyyppi ja käyttämä portti, jos asennat kirjoittimen mikroon paikallisesti
- Korvataanko mahdollisesti aikaisempi mikrossa oleva käyttöjärjestelmä Windows NT:llä vai käytetäänkö Windows NT:n dual-boot-ominaisuutta. Haluttaessa esimerkiksi samaan mikroon Windows 95 ja Windows NT on C:-asemaan **ennen** NT:n asentamista asennettava **MS-DOS** ja **FAT** -tiedostojärjestelmä. Tämän jälkeen voidaan asentaa joko Windows 95 tai Windows NT. - Tähän tulisi olla jokin erityinen syy, koska en suosittele palvelimeen muuta kuin NT-käyttöjärjestelmää!

Asetuksia, joita **et voi muuttaa asennuksen jälkeen ilman NT:n uudelleenasennusta**, ovat ainakin seuraavat:

- **Palvelimen rooli** - ohjauskone (Domain Controller)-tyyppinen palvelin on **aina** ohjauskone (Domain Controller)-tyyppinen palvelin. PDC:n voi muuttaa BDC:ksi **Server Manager**-ohjelmalla, mutta **Stand-alone Server**-tyyppistä palvelinta ei voi muuttaa ohjauskone (Domain Controller)-tyyppiseksi palvelimeksi!



- Em. menetelmä on hyödyllinen korjattaessa PDC:tä tai lisättäessä muistia PDC:iin. Hätätilanteessa voi asentaa vaikkapa ensin työaseman BDC:ksi ja sitten vaihtaa sen roolin PDC:ksi, kunnes alkuperäinen PDC voidaan palauttaa verkkoon. Tällöin roolit taas muutetaan

- **Stand-alone Server**-tyyppisen palvelimen voi siirtää toiseen toimialueeseen, mutta siinäkin se voi olla vain **Stand-alone Server**-tyyppinen palvelin

- Ohjauskone (Domain Controller)-tyyppisen palvelimen voi *ehkä* pystyä siirtämään toiseen toimialueeseen, mutta siirtäminen saattaa edellyttää NT:n uudelleenasentamista kyseiseen palvelimeen

- NT:n järjestelmäosion (WINNT-hakemisto alihakemistoineen) koko ja sijainti. Järjestelmäosio voi olla FAT tai NTFS, mutta pyri kuitenkin suosimaan NTFS:ää sen mahdollistamien suojausten vuoksi. Järjestelmäosio voi sijaita esim. D:-asemassa. Työasemassa, jossa on esim. yksi 1 Gt levy, kannattanee jättää yksi levyosio (esim. C:), jolla on järjestelmäosion lisäksi sekä käyttäjän sovellukset että datatiedostot. Palvelimessa tilanne on hieman eri

- Koska järjestelmäosion koko ja sijainti määritellään asennusvaiheessa, suosittelen heti asennusvaiheessa varaamaan järjestelmäosiolle riittävästi levytilaa (300 Mt - 500 Mt). Järjestelmäosion levytilaa vievät:

  - Uudet ohjelmistot ja asennettavat ominaisuudet, niiden DLL:t ja EXE:t vievät levytilaa

  - **Sivutustiedostolle** (Pagefile.sys) on syytä varata järjestelmäosiolla ainakin RAM + 12 Mt kooltaan oleva sivutustiedosto NT:n elvytystoimintoja varten

  - **Service Packien** asennukset edellyttävät vapaata levytilaa (noin 50 - 60 Mt) - jos levy on täynnä, et voi asentaa Service Packejä!

  - Oletuksena **tulostusjonot** luodaan järjestelmäosiolle - sen voi muuttaa kirjoittimien asetuksista tai rekisteristä (rekisteristä tulostusjonojen muuttaminen oli ainoa mahdollisuus NT 3.5x:ssä).

Windows NT 4.0 Server CD-ROM

Windows NT 4.0 Serverin CD-ROM:in hakemistorakenne on seuraavanlainen.

Asennushakemistot eri prosessoriperheille:

ALPHA	DEC Alpha
I386	Intel i386 (i486, Pentium jne)
MIPS	MIPS
PPC	PowerPC

A.o. hakemiston alla ovat seuraavat:

DRVLIB.NIC	Ajuri-yms. hakemistoja
INETSRV	Internet Information Server
NETMON	Verkkomonitori
SYSTEM32	Mm. tuki buuttaavalle CD-ROM:ille

Tukihakemistot:

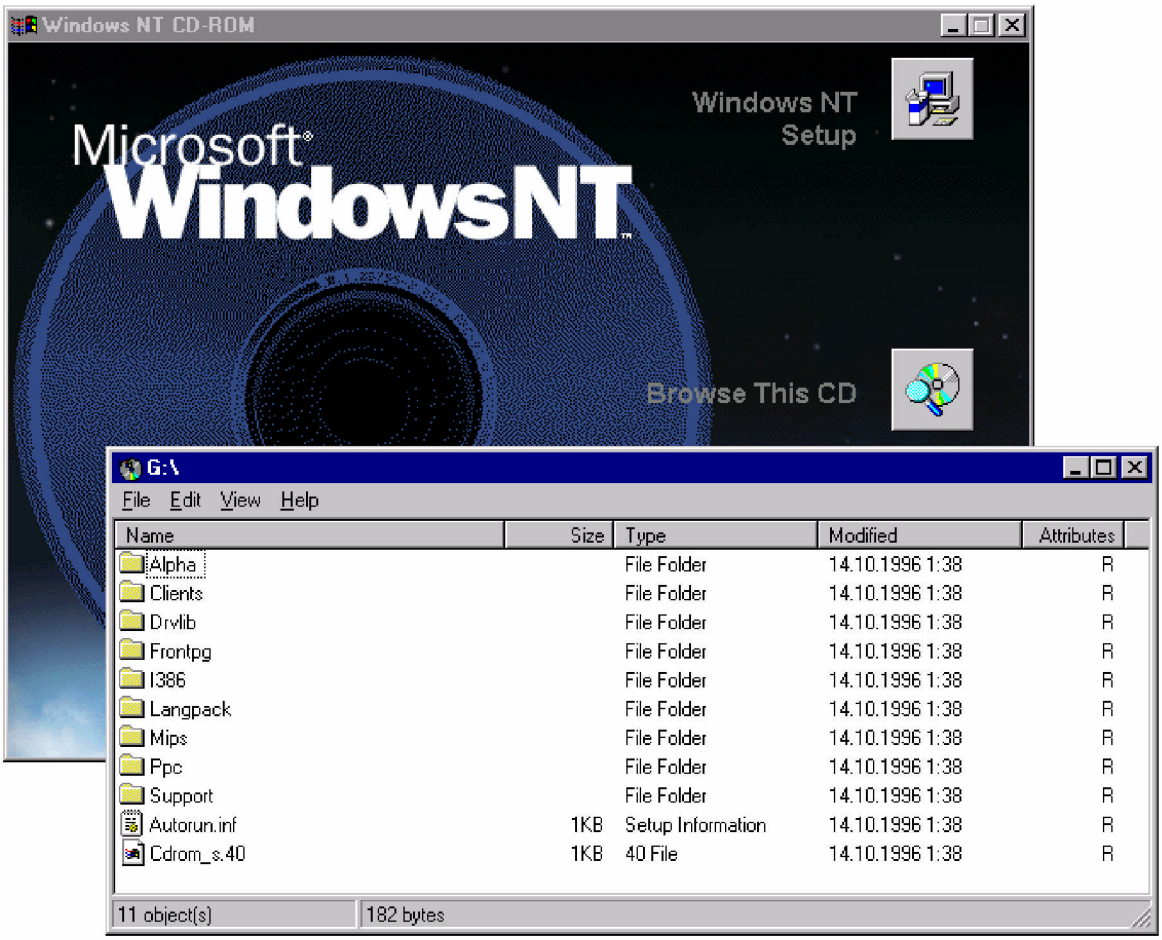
CLIENTS	Työasemahakemistot
DRVLIB	Ajuri-yms. hakemistoja
FRONTPG	FrontPage
LANGPACK	Kielituki
SUPPORT	Käsikirjat ja *Yhteensopivien laitteiden luettelo* (Hardware Compability List, HCL)

Edellisen CLIENTS-hakemiston alla ovat seuraavat:

LANMAN	LM (DOS)
LANMAN.OS2	LM (OS/2)
MSCLIENT	MS Network Client (DOS)
RAS	RAS-tuki (DOS)
RPL	Etäkäynnistystuki
SRVTOOLS	NT-palvelimen hallintaohjelmat (Windows NT 4.0-työasema ja Windows 95)
SUPPORT	Windows95-asennustiedostojen kopiointi NT-palvelimelle
TCP32WFW	MS TCP/IP-32b (WfW)
UPDATE.WFW	WfW:n päivitystiedostoja
WIN95	Windows95 (US)

CLIENTS\SRVTOOLS-hakemiston alla ovat seuraavat hallintaohjelmien asennushakemistot:

WIN95	Windows95-versio
WINNT	Windows NT 4.0



Asennusohjelman suoritus

Miten käynnistät asennusohjelman riippuu siitä, mistä ja miten asennat NT:n.

Seuraavassa käsitellään NT-palvelimen perusasennusta: korjauspäivitykset (*Service Pack*) ja versiopäivitykset on käsitelty myöhemmin.

Jos asennus ei ole sinulle täysin tuttua, tutustu seuraaviin asennusvaihtoehtoisihin ja asennusohjelman eri vaiheisiin. Aloittelevalle NT-managerille suosittelen **CD-ROM-asennusta** paikallisesta CD-ROM-asemasta.

Toinen menetelmä on **WINNT.EXE**- tai **WINNT32.EXE**-asennusohjelmien käyttö. **WINNT.EXE** on tarkoitettu asennukseen MS-DOS-mikrossa ja **WINNT32.EXE** on tarkoitettu päivitykseen aikaisemman version Windows NT-mikrossa.

CD-ROM

Helpointa ja turvallisinta palvelimen asennus on paikallisen CD-ROM-aseman avulla. Jos se on tuettu (ks. HCL, Hardware Compability List) CD-ROM-asema (**SCSI**, **ATAPI**), niin aseta NT:n CD-ROM-levy asemaan, **Setup Boot Disk-levyke A:-asemaan** ja käynnistä mikro. Katso ohjeita hieman edempää tässä luvussa.

Setup Boot Diskin ja asennuslevykkeiden on oltava nimenomaan tarkoitetut palvelimen CD-ROM-asennukseen! Tällaiset levykkeet voit tarvittaessa luoda palvelimen CD-ROM:in prosessorikohtaisesta asennushakemistosta (esimerkiksi **i386**) komennolla **WINNT /OX**. Toimii DOS- ja Windows 95-mikroissa.

Huomattavaa:

- Windows NT 4.0 tukee myös **ATAPI**- eli ns. Enhanced IDE-CD-ROM -asemia. Palvelimessa en suosittelisi käyttämään, koska niistä *saattaa* aiheutua ongelmia

- Kiintolevyn ei tarvitse CD-ROM-asennuksessa olla alustettu eikä edes osioitu, vaan asennusohjelma antaa mahdollisuuden tehdä osioinnin ja alustuksen asennuksen yhteydessä.

Verkko

Voit myös käynnistää asennusohjelman komennolla **WINNT** verkon jaetusta hakemistosta (minne CD-ROM on kopioitu) tai verkkoon jaetusta CD-ROM-asemasta hakemistosta **i386**. Tällöin tarvittavat asennuslevykkeet luodaan asennusohjelman ajon aikana ja tiedostot kopioidaan paikalliselle kiintolevylle, ja mikro käynnistetään uudelleen **Setup Boot Disk**-levykkeellä. Kiintolevyn on oltava alustettu MS-DOS:in tukemalla FAT-tiedostojärjestelmällä ja sillä on oltava vähintään 160 Mt vapaata levytilaa.

Huomattavaa:

- Voit tehdä verkkokäynnistyslevykkeen palvelimen Network Client Administrator -ohjelmalla. Käynnistämällä asennettavan mikron tällaisella käynnistyslevykkeellä, pääset kirjoittautumaan suoraan verkkoon ja käyttämään verkon resursseja ilman, että verkkokäynnistysjärjestelmän työasemaosaa tarvitsisi asentaa asennettavan mikron kiintolevylle.

- Voit myös kopioida tiedostot CD-ROM:in **i386**-hakemistosta paikalliselle kiintolevylle esim. **i386-**hakemistoon ja käynnistää asennusohjelman sieltä.

- Kaikissa tapauksissa käytettyjen SCSI-ohjainten ja -oheislaitteiden terminoinnin on syytä olla oikein!

Muita tunnettuja tai vähemmän tunnettuja vaihtoehtoja ovat seuraavat:

1) Verkkopalvelimen jakamasta **NT:n asennus-CD-ROM-levyltä**. Palvelin voi olla hyvinkin vaatimaton eli **Työryhmä-Windows** (Windows for Workgroups, WfW) tai **Windows 95**-mikro. WfW-mikrot voivat jakaa CD-ROM-asemiaan asetuksella **MSCDEX /S**. Myös **Add-On for DOS**-mikron tai **Novell NetWare**-palvelimen jakama hakemisto käy jne.

Tämän jälkeen tarvitset **verkkokäynnistyslevykkeen**, jolla voit käynnistää asennettavan mikron verkkoon. Ota yhteys palvelimelta jaettuun CD-ROM:in **i386**-hakemistoon ja anna komento **WINNT**. Ongelmallisissa tilanteissa voit joutua antamaan eräitä valitsimia, kuten viittaus asennusohjelman käyttämään väliaikaiseen hakemistoon **/T**.

Voit myös kopioida asennustiedostot palvelimen jakamasta CD-ROM:ista paikalliselle kiintolevylle. Tämä on suositeltavaa silloin, jos asennusohjelma jumiutuu jatkuvasti yrittäessään käynnistää verkkoa. Kopioi prosessorikohtainen hakemisto (esim. **i386**) kokonaisuudessaan (mutta ei *välttämättä* verkkokorttien hakemistoa **DRVLIB.NIC**)!

2) Verkosta eli **verkon levyasemalle kopioidusta NT:n asennus-CD-ROM-levystä**. Kopioi verkon jaettuun hakemistoon NT:n CD-ROM (työasema/palvelin); Intel-ympäristössä minimissään käytettävät tiedostot löytyvät CD-ROM:in **i386**-hakemistosta eli kopioi se CD-ROM:ilta palvelimen jaettuun hakemistoon, mutta ei *välttämättä* verkkokorttien hakemistoa **DRVLIB.NIC**!

Tämän jälkeen tarvitset työasemassa **verkkokäynnistyslevykkeen,** jolla voit käynnistää asennettavan mikron verkkoon. Ota yhteys palvelimen jaettuun hakemistoon, siirry tarvittaessa oikeaan hakemistoon ja anna komento **WINNT**. Ongelmallisissa tilanteissa voit joutua antamaan eräitä valitsimia, kuten määrittelemään väliaikaisen hakemiston valitsimella **/T**.

Voit myös kopioida asennustiedostot palvelimelta. Tämä on suositeltavaa silloin, jos asennusohjelma jumiutuu jatkuvasti yrittäessään käynnistää verkkoa.

3) Voit asentaa suoraan CD-ROM-levyltä **WINNT**-komennolla. Ongelmallisissa tilanteissa voit taas joutua antamaan eräitä valitsimia. Tällöin NT:stä ei tarvitse löytyä tukea käytettävälle CD-ROM:ille, koska asennustiedostot joka tapauksessa kopioidaan kiintolevylle. Käynnistä mikro MS-DOS:iin CD-ROM:in tuella ja aja sen jälkeen NT:n asennusohjelma.

4) Edellä tulikin jo esille se, että kiintolevylle kopioidulta NT:n CD-ROM-levyltä voidaan myös ajaa asennus. Ongelmia kohdattaessa voidaan jälleen käyttää sopivia parametreja, esimerkiksi käytettävä komento voi olla **WINNT /S:C:\i386 /T:C: /X.** /S määrittelee asennusohjelmien sijaintihakemiston.

5) Eräillä valmistajilla on omia ratkaisujaan - esimerkiksi **Compaqilla SmartStart**, jolloin asennuksessa on syytä noudattaa laitevalmistajan ohjeita NT:n asennuksessa

6) *Unattended Setup* on asennusmenetelmä, jolloin voidaan käyttää ennalta luotua **asennuskriptiä** eli **vastaustiedostoa** (*Answer File*). Ks. esimerkiksi i386-hakemiston **UNATTEND.TXT**.

Sellaisen voit luoda Windows NT 4.0 Serverin CD-ROM:illa tulevalla **Windows NT Setup Managerilla**. Ohjelma on hakemistossa **Support\Deptools**. Komento on tällöin perusasennuksessa esimerkiksi **WINNT /U:C:\UNATTEND.TXT /S:X: /B**, jolloin käytetään C:-aseman juurihakemistossa olevaa skriptiä ja asennetaan **X:**-asemasta. **/B** asentaa käynnistystiedostot kiintolevylle, jolloin käynnistyslevykkeitä ei tarvita. Päivitys suoritettaisiin komennolla **WINNT32 /U:C:\WS3\UPGRADE.TXT /S:I:\I386 /B**, joka etsii skriptiä **c:\ws3** -hakemistosta.

Asennuksessa käytetään I:-aseman i386-hakemistoa. **/B** asentaa käynnistystiedostot kiintolevylle, jolloin käynnistyslevykkeitä ei tarvita. Katso esimerkkejä myöhemmin tässä kirjassa.

WINNT- ja WINNT32-komennot

Jos haluat asentaa verkosta (ts. verkon levyasemalle kopioidusta CD-ROM-levystä) tai suoraan CD-ROM-levyltä, kiintolevylle kopioidusta NT:n CD-ROM-levystä tai CD-ROM-asemasta, jota NT ei tue, siirry i386-hakemistoon ja anna komento **WINNT**.

Asennusohjelman valitsimet ovat:

WINNT [/D[:]winntroot] [/S[:]sourcepath] [/T[:]tempdrive] [/I[:]inffile] [/O[X]] [/X | [/F] [/C]] [/B]

/D[:]winntroot	poistaa NT:n järjestelmätiedostot ennen asennusta annetusta hakupolusta, esim. **C:** (*ei NT 3.51:ssä*)
/S[:]sourcepath	määrittelee mistä NT:n asennustiedostot löytyvät. Oletus on nykyinen hakemisto
/T[:]tempdrive	määrittelee levyaseman, jonne asennuksessa käytettävät väliaikaistiedostot sijoitetaan. Oletuksena NT etsii sopivimman, esim. **C**:n. Joissakin mikroissa tämä asetus kannattaa mainita - varsinkin, jos C:-asemassa on esimerkiksi valmistajan diagnostiikka/asennusapuohjelmia eli C:-asemassa on osioimaton levyalue
/I[:]inffile	asennuksen käyttämän asetustiedoston nimi. Oletus on **DOSNET.INF**
/O	luodaan vain asennuksen käyttämät levykkeet
/OX	luodaan levykkeet CD-ROM- tai levykeasennukselle
/X	ei luoda asennuksen käyttämiä levykkeitä
/F	ei verifioida asennuslevykkeiden luontivaiheessa niille kopioitavia tiedostoja
/C	ohita levykkeiden vapaan tilan tarkistus
/B	levykkeetön asennus. **/B** asentaa käynnistystiedostot kiintolevylle, jolloin käynnistyslevykkeitä ei tarvita

Lisäksi on käytettävissä asennus ennalta tehdyn asennusta ohjaavan skriptin avulla - tämä tehdään valitsimella **/U**. Valitsimia voi käyttää samanaikaisesti useitakin, esimerkiksi:

```
WINNT /S:C:\i386 /T:C: /X
```

Päivitystä ei tehdä samalla komennolla. **Versiopäivitys Windows NT 3.51:stä versioon 4.0** suoritetaan komennolla **WINNT32**:

- Windows NT Workstation -työasemat voidaan päivittää Server-tyyppisiksi palvelimiksi (*Server*), mutta ei toimialueen **ohjauskoneiksi** (PDC tai BDC).

Jos haluat asentaa **korjauspäivityksen** (*Service Pack*), niin se suoritetaan komennolla **UPDATE.EXE**. Eri laitevalmistajilla on lisäksi omia päivityksiään (esimerkiksi Compaqilla **System Support**-päivitykset), joten on syytä ennen korjauspäivitystä tutustua laitevalmistajan suosituksiin korjauspäivitysten asentamisessa.

Käytettävissä olevat komentorivin komennot ovat siis tilanteesta ja asennettavasta NT-versiosta riippuen:

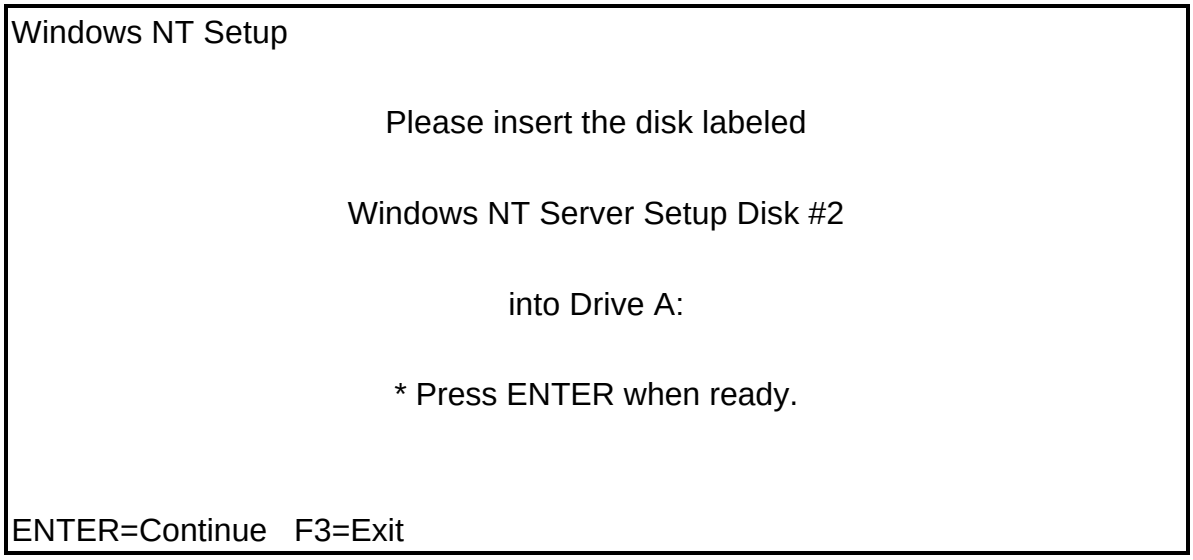
WINNT	Perusasennus (palvelin tai työasema). Ohjelmatiedosto on **WINNT.EXE**
WINNT32	Versiopäivitys (palvelin tai työasema). Ohjelmatiedosto on **WINNT32.EXE**
UPDATE	Korjauspäivitys eli **Service Pack**, samassa paketissa on palvelin- ja työasemaversio. Ohjelmatiedosto on **UPDATE.EXE** - **korjauspäivitys on kieliversiokohtainen!**

Palvelimen asentaminen

Kuten aiemmin todettu, NT-työaseman asennus on varminta paikallisen CD-ROM-aseman avulla. Sen olisi hyvä olla SCSI-CD-ROM, mutta ei välttämättä. Palvelimessa tulisi kuitenkin käyttää vain SCSI-kiintolevyjä. Syynä on suorituskyky ja toimintavarmuus.

1) Jos CD-ROM-asema on tuettu (ks. HCL, *Hardware Compability List*) tai ATAPI 1.2-määritystä noudattava, niin aseta NT:n CD-ROM-levy asemaan, **Setup Boot Disk**-levyke A:-asemaan ja käynnistä mikro. Jos saat virheilmoituksen CD-ROM:illa sijaitsevasta tiedostosta, poista Windows NT:n CD-ROM-levy toistaiseksi asemasta ja käynnistä mikro uudelleen.

2) Vaihda pyydettäessä **levyke 2** (Setup Disk 2) asemaan.



3) Tämän jälkeen näyttöön tulee **Welcome to Setup**.

```
Windows NT Server Setup

Welcome to Setup.

The Setup program for the Microsoft (R) Windows NT (TM) operating system
version 4.0 prepares Windows NT to run on your computer.

  •To learn more about Windows NT Setup before continuing, press F1.

  •To set up Windows NT now, press ENTER.

  •To repair a damaged Windows NT version 4.0 installation, press R.

  • To quit Setup without installing Windows NT, press F3.


ENTER=Continue   R=Repair   F1=Help   F3=Exit
```

Valitse:

- **F1** - opaste
- **ENTER** - asennus
- **R** - korjauslevykkeen avulla voit yrittää korjata vaurioitunutta NT:tä
- **F3** - lopetus

Paina **ENTER.**

4) Seuraavaksi suoritetaan kiintolevyjen ja muiden massamuistien sekä niiden NT:n mukana tulevien ohjainten tarkistus. Jos painetaan **ENTER**, niin NT etsii NT:n mukana tuetut massamuistiohjaimet. Joissakin mikroissa asennus saattaa jumiutua tähän - selvitä silloin massamuistiohjainten tarkka tyyppi ja ohita tämä vaihe **S**:llä. Jos sinulla on laitevalmistajan tukilevyke, jolta ohjain löytyy, paina myös silloin **S**. Muuten kannattaa painaa tässä **ENTER**.

Windows NT Server Setup

Setup automatically detect floppy disk controllers and standard ESDI/IDE hard disks without user intervention. However on some computers detection of certain other mass storages, such as SCSI adapters and CD-ROM drives, can cause the computer to become unresponsive or to malfunction temporarily.

For this reason, you can bypass Setup's mass storage device detection and manually select SCSI adapters, CD-ROM drives, and special disk controllers (such as drive arrays) for installation.

•To continue, press ENTER.
Setup will attemp to detect mass storage devices in your computer.

•To skip mass storage detection, press S.
Setup will allow you to manually select SCSI adapters, CD-ROM drives, and special disk controllers for installation.

F3=Exit ENTER=Continue S=Skip Detection

5) Asenna pyydettäessä **levyke 3** (Setup Disk 3) asemaan ja paina **ENTER**. Asennusohjelma tutkii ja ilmoittaa etsinnän aikana löytyviä ohjaimia.

Windows NT Server Setup

Please insert the disk labeled

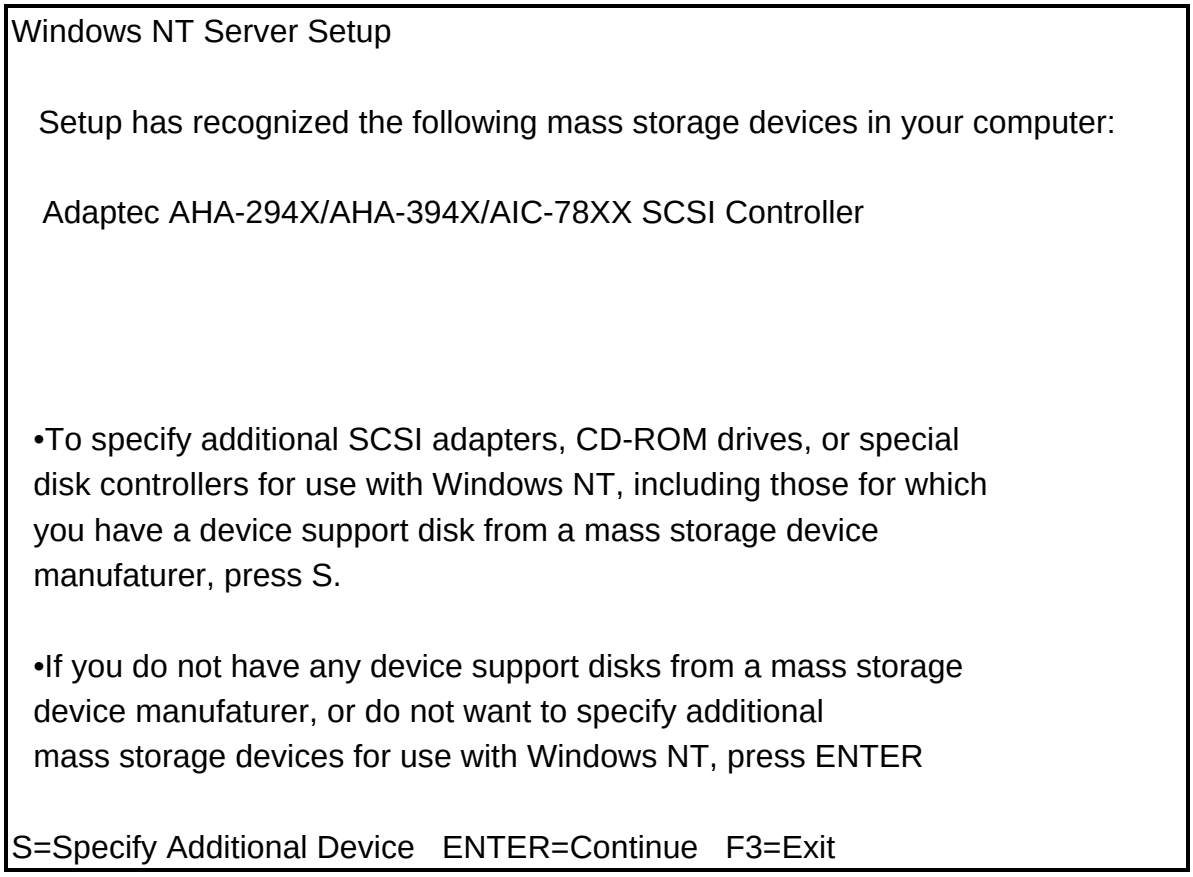
Windows NT Server Setup Disk #3

into Drive A:

* Press ENTER when ready.

ENTER=Continue F3=Exit

Lopuksi saat listan löydetyistä massamuistiohjaimista.



6) Jos tiedät, että tarvitset muun kuin NT:n mukana tulevan SCSI- tai muun kiintolevyn / CD-ROMin ohjaimen, voit vielä tässä vaiheessa painaa **S**. Jos luettelo on oikea, kannattaa jatkaa painamalla **ENTER**. Tällöinkin voit myöhemmin asentaa tarvittaessa lisää ohjaimia.

Huomaa:

- Jos mikrossasi on useampia ohjaimia kuin asennusohjelman löytämät tai jos asennusohjelma ei löytänyt yhtään ohjainta, ja mikrossasi sellainen kuitenkin on, valitse tässä vaiheessa **S** (Specify Additional Device) eli asenna lisää ohjaimia. Tällöin saat näyttöön listan ohjaimista.

- Jos mikroon asennettu ohjain ei ole luettelossa, vaikka se löytyy NT:n tukemien ohjainten listasta, niin on syytä epäillä kyseisen ohjaimen asetuksia (IRQ jne).

- Jos käyttämäsi ohjain ei ole luettelossa, tarvitset valmistajan NT-ohjaimen. Valitse tällöin **Other**, minkä jälkeen voit asettaa esimerkiksi valmistajan tukilevykkeen A:-asemaan ja painaa **ENTER**. Riippuen valmistajasta näyttöön saattaa tulla lista useistakin ohjaimista; valitse oikea ja paina **ENTER**. Tämän jälkeen palataan edelliseen näyttöön.

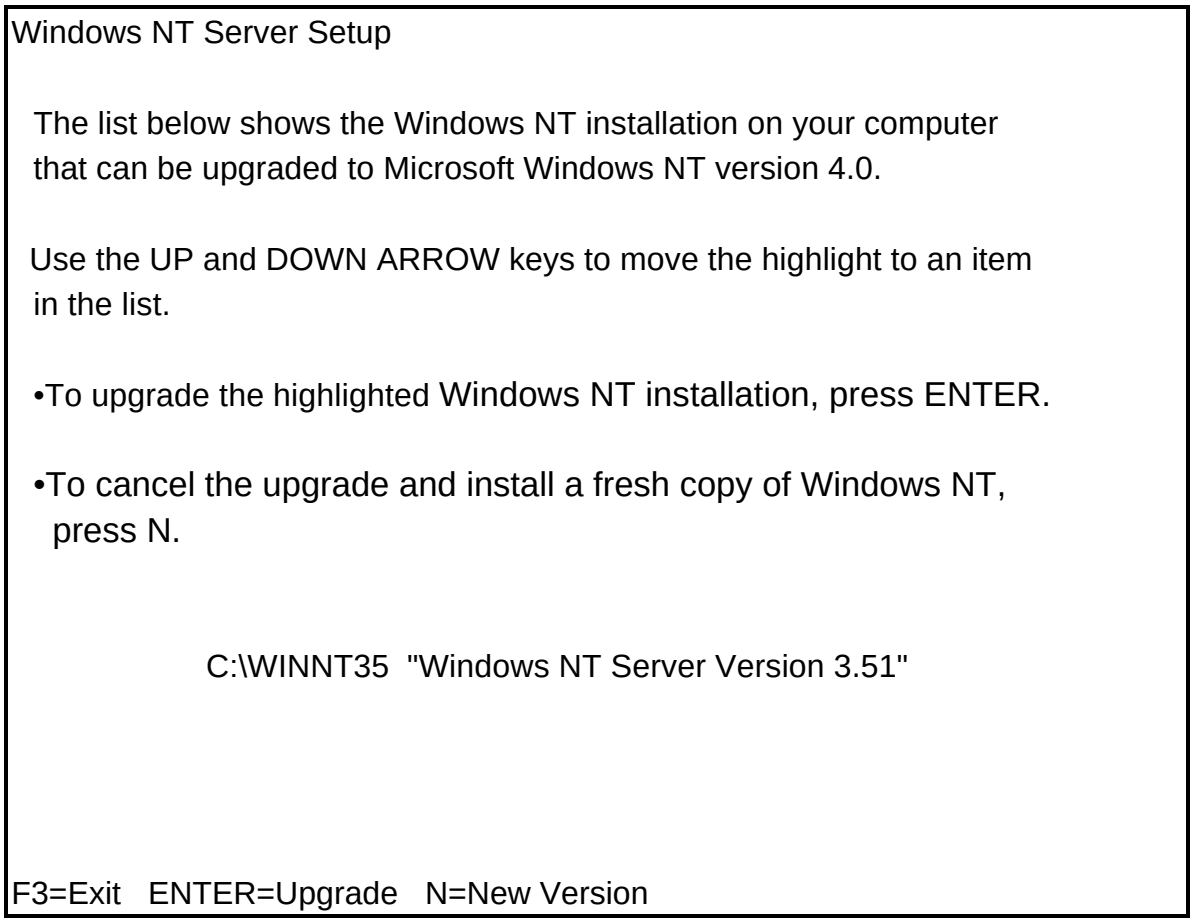
- NT ei kuitenkaan käynnisty, jos kiintolevyn ohjainta ei ole asennettu jo tässä vaiheessa.

- Jos CD-ROM on puuttuvan tai väärin määritellyn ohjaimen takana, ei asennusohjelma voi jatkaa CD-ROM:ilta. Tällöin ei myöskään vaihtoehto NT:n asentamiseksi CD-ROM-levyltä ole käytettävissä.

Muuten **ENTER** jatkaa normaalisti eteenpäin. Tarvittaessa asennus voidaan lopettaa painamalla **F3**.

Tässä vaiheessa tulee lisenssisopimuksen ehdot. Paina **PageDown** (kahdeksan kertaa) ja **F8** (I Agree).

7) Jos palvelimessa on jokin aiempi NT-versio asennettuna, asennusohjelma kysyy tarvittaessa, asennetaanko mahdollisesti **aiemmin asennetun NT:n hakemistoon** (esim. **C:\WINNT** tai **C:\WINNT35**).



Tällöin laitteistoasetukset luetaan aiemmin tehdystä asennuksesta ja voit siirtyä laitteistoasetuksiin eli katso valinnat tarkemmin edempänä. Samoin tapahtuu, jos kiintolevyllä ei ollut aiempaa NT-asennusta eli tällöinkin voit siirtyä eteenpäin **määriteltäviin laiteasetuksiin**.

Valitse päivitys painamalla **ENTER**. Voit asentaa uuden asennuksen painamalla **N**.

8) Seuraavaksi esitellään laiteasetukset.

```
Windows NT Server Setup

  Setup has determined that your computer contains the following hardware
  and software components.

          Computer: Standard PC
            Display: VGA or Compatible
           Keyboard: XT, AT, or Enhanced Keyboard (83-102 keys)
  Keyboard Layout: Finnish
    Pointing Device: Microsoft Serial Mouse

         No Changes: The above list matches my computer.

  If you want to change any item in the list, press the UP or DOWN ARROW
  key to move the highlight to the item you want to change. Then press
  ENTER to see alternatives for that item.

  When all items in the list are correct, move the highlight to
  "The above list matches my computer" and press ENTER.


ENTER=Select   F3=Exit
```

Huomaa, että laitetyypin (Computer) valinnoissa on omat vaihtoehtonsa moniprosessorimikroille. Jos käytät moniprosessorikelpoista mikroa yhdellä prosessorilla, valitse mikron tyypiksi **MPS Uniprocessor PC**. Jos asennus ei jostain syystä aiemmin onnistunut, kokeile asentamalla **Standard PC**. **Pentium** ja **Pentium Prot** ovat **Standard PC**.

Vaihda asetukset tarvittaessa haluamiksesi; esimerkiksi **Keyboard Layout** kannattanee vaihtaa **Finnish**-versioksi siirtymällä oletuksena olleen **US**:n päälle, painamalla **ENTER** ja selaamalla listasta **Finnish**.

Tarkista, että hiiri on löytynyt.

9) Asennusohjelma kysyy seuraavaksi, minne levyosioon NT asennetaan.

Windows NT Server Setup

The list below shows existing partitions and spaces available for creating new partitions.

Use the UP and DOWN ARROW keys to move the highlight to an item in the list.

- To install Windows NT on the highlighted partition or unpartitioned space, press ENTER.
- To create a partition in the unpartitioned space, press C.
- To delete the highlighted partition, press D.

2040 MB Disk 0 at Id 0 on bus on aic78xx

C: New (Unformatted) 2040 MB

2040 MB Disk 0 at Id 1 on bus on aic78xx

D: NTFS (FISHWARE) 2039 (1037 MB free)

ENTER=Install D=Delete Partition F1=Help F3=Exit

Valitse sopiva levyosio:

- Oletus on C:-asema (SCSI-levyllä ilmoitus on esim. **Disk 0 at Id 0 on bus 0 on aic78xx**; myös tiedostojärjestelmän tyyppi ilmoitetaan, esim. **FAT** tai **NTFS**), levyosion nimi (esimerkissä D:-aseman nimi on **FISHWARE**) sekä vapaa levytila.

- Jos haluat asentaa toistaiseksi osioimattomalle kiintolevyn osalle, valitse **C**.

- Tarvittaessa voit poistaa jonkin osion painamalla **D**.

Huomaa:

- NT:n järjestelmäosio voi olla FAT tai NTFS, mutta pyri kuitenkin suosimaan NTFS:ää sen mahdollistamien suojausten vuoksi. Koska järjestelmäosion koko ja sijainti määritellään asennusvaiheessa, suosittelen heti asennusvaiheessa varaamaan järjestelmäosiolle riittävästi levytilaa (300 Mt - 500 Mt)

- Jos kiintolevy on fyysisesti vahingoittunut, NT:n asennusohjelma saattaa löytää sen, mutta asennus ei silti onnistu

- SCSI-laitteiden terminoinnin on myös syytä olla oikein.

10) Valitse tiedostojärjestelmä.

Seuraavaksi tehdään valinnat osion suhteen:

```
If you want to select different partition for Windows NT, press ESC.

Format the partition using the FAT file system
Format the partition using the NTFS file system
Convert the partition to NTFS
Leave the current file system intact (no changes)
```

Valinnat ovat seuraavat:

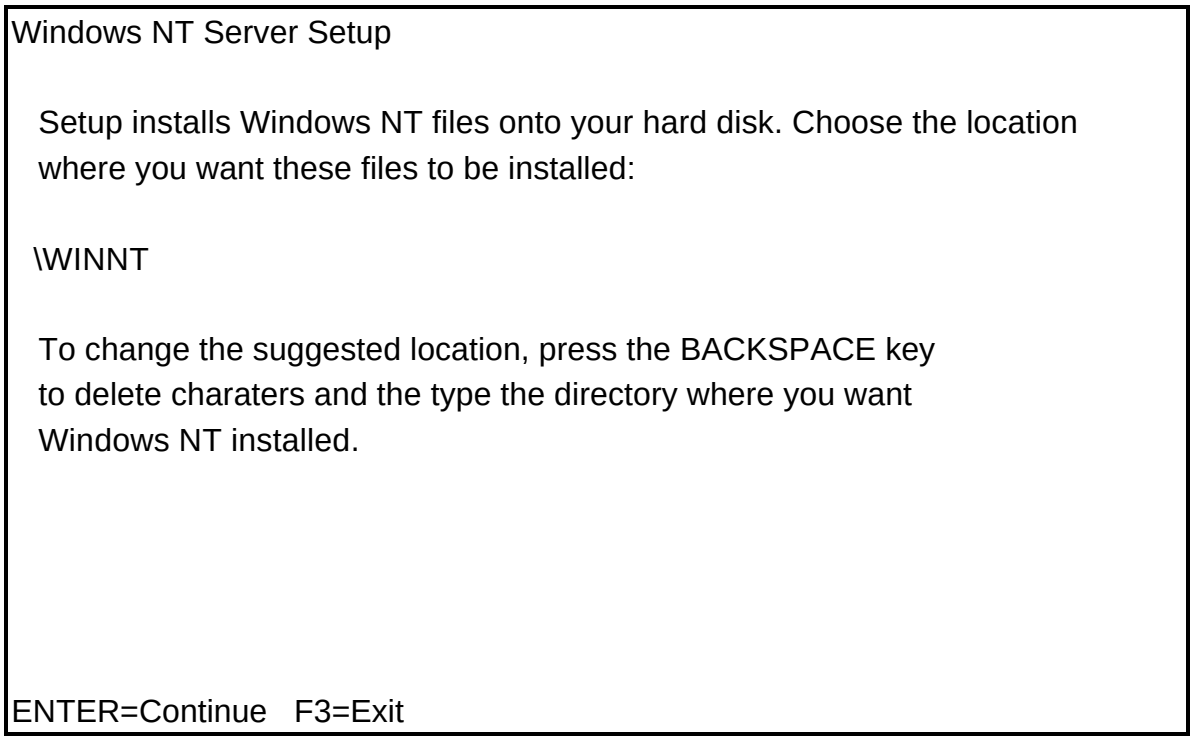
- **Format the partition using the FAT file system** - alustetaan levyosio FAT-tiedostojärjestelmällä
- **Format the partition using the NTFS file system** - alustetaan levyosio NTFS-tiedostojärjestelmällä
- **Convert the partition to NTFS** - muunnetaan levyosio NTFS-tiedostojärjestelmään
- **Leave the current file system intact (no changes)** - ei tehdä muutoksia
- **ESC** - peruutus

Tee valinta. Ehkä sopivin on **Convert the partition to NTFS**, jos haluat käyttää heti NTFS:n ominaisuuksia. Jos otat tai jätät FAT:in käyttöön, myöhemmin voit tehdä muunnoksen **CONVERT**-ohjelmalla. FAT:ista voi olla etua, jos sinulla on ongelmia asentaa NT:tä kyseiseen mikroon ja joudut käynnistämään mikron DOS-käynnistyslevykkeellä päästäksesi käsiksi järjestelmäosioon. FAT:in käyttöönotto on myös hieman nopeampi kuin NTFS:n, mutta se mahdollista mitään suojauksia järjestelmäosioon.

Asennusohjelman tarjoama oletus voi olla esimerkiksi **Leave the current file system intact (no changes)** eli ei tehdä muutoksia tiedostojärjestelmään. Jos valitsit **Format the partition using...** alustus alkaa painamalla seuraavaksi käytettävissä olevista valinnoista riippuen joko **ENTER** tai **F**; **ESC** peruuttaa.

Tällöin myös kerrotaan, mikä alustetaan.

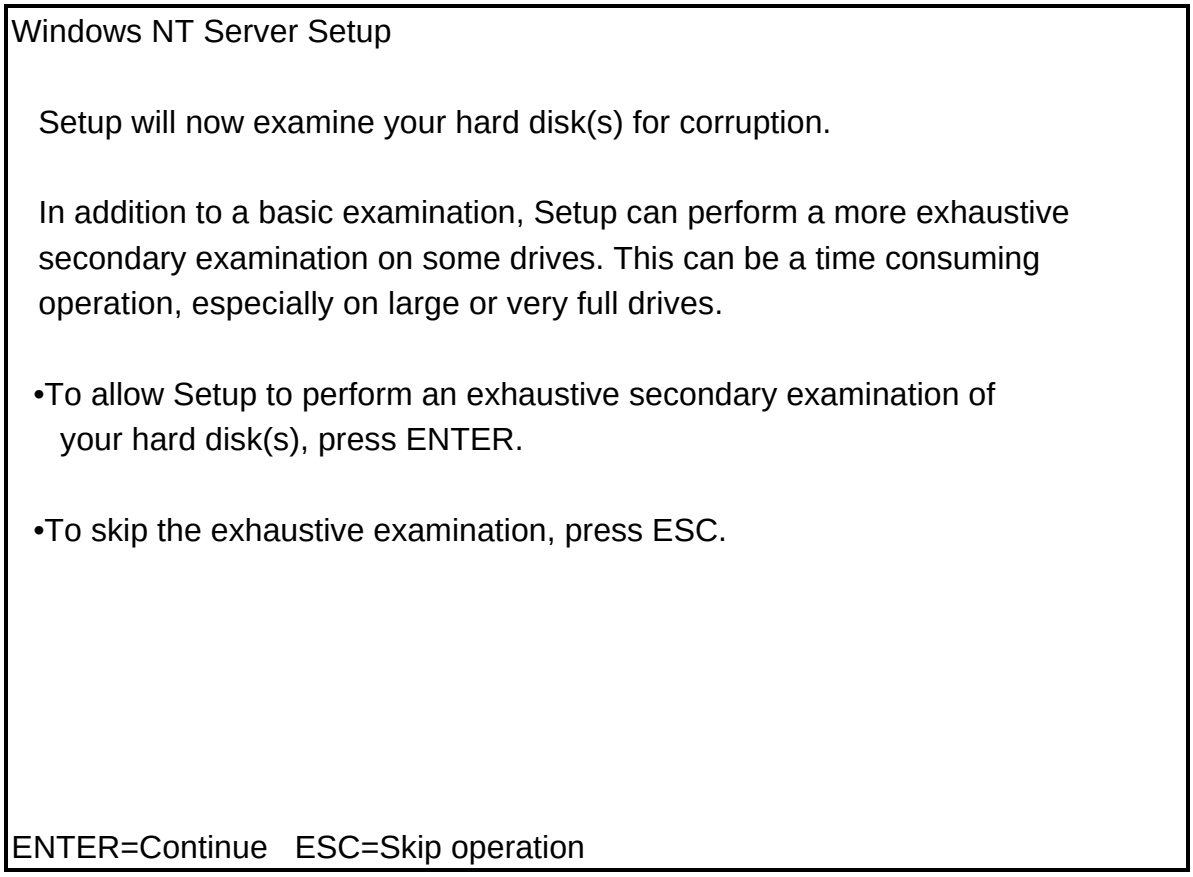
11) Seuraavaksi asennusohjelma kysyy minne asennetaan.



Oletus on **WINNT**:

- **ENTER** - asennus tarjottuun hakemistoon - tällöin voidaan suorittaa vaikkapa päivitys aiemmasta NT-versiosta (esimerkin kuvassa)
- **PALAUTUSNÄPPÄIN** (BACKSPACE) - voit korjata hakemiston nimen
- Joissakin tilanteissa myös: **N** - voit antaa toisen hakemiston.

12) Tämän jälkeen tarjotaan mahdollisuutta tarkistaa kiintolevyn kunto.

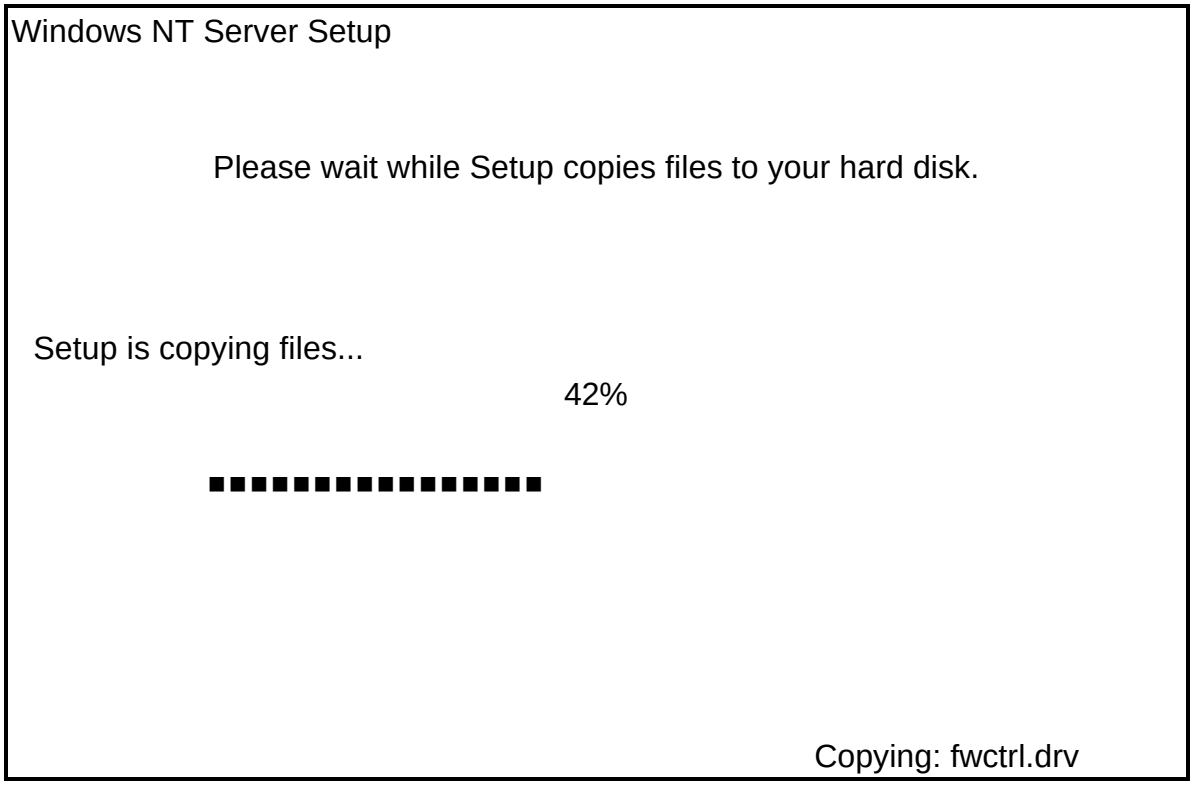


Valinnat ovat seuraavat:

- **ENTER** suorittaa tarkistuksen (Exhaustive)
- **ESC** ohittaa.

Tutkitaan kiintolevy painamalla **ENTER**. Tämän jälkeen asennusohjelma saattaa pyytää laitevalmistajan tukilevykkeitä.

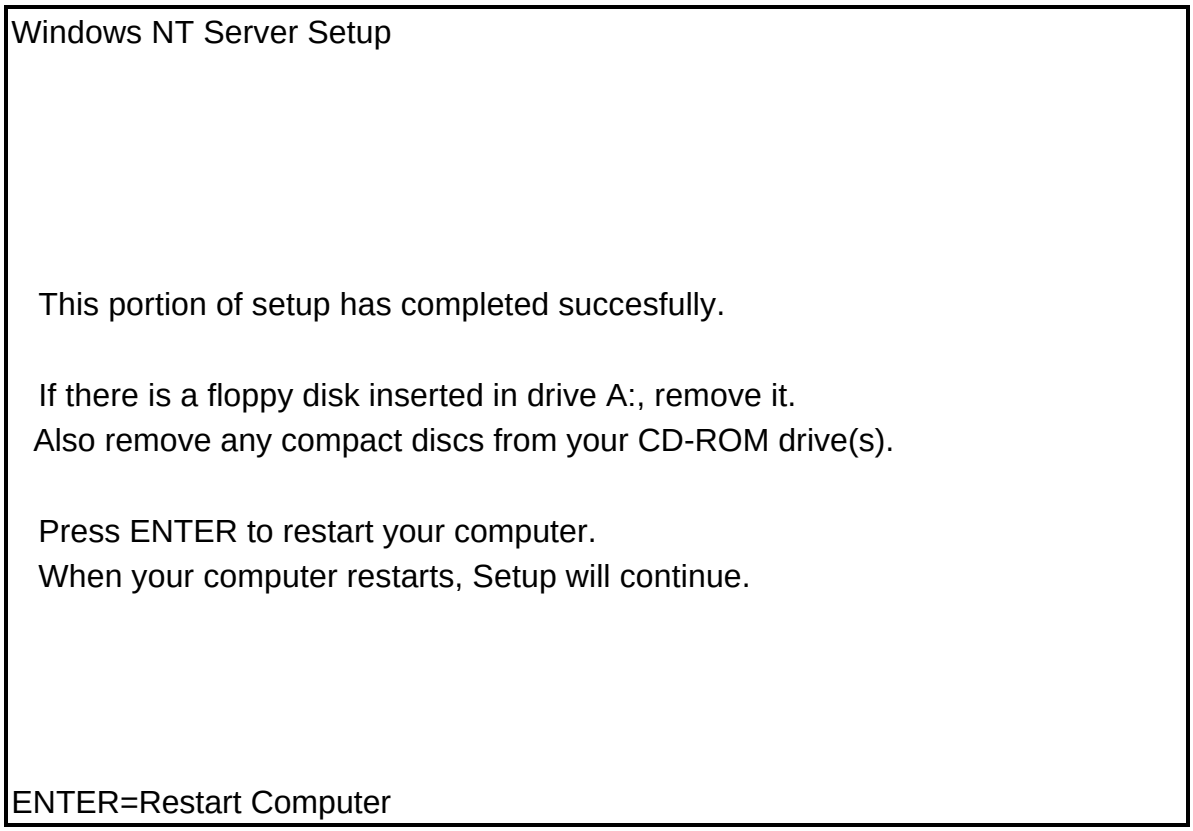
Seuraavaksi asennusohjelma kopioi tiedostot kiintolevylle. Tällöin näytössä on keltainen palkki sekä prosentit kopioinnin edistymisestä. Oikeassa alanurkassa näet kopioitavan tiedoston nimen.



Jos tässä vaiheessa tulee virheilmoituksia, ettei tiedostoa voida kopioida (Setup cannot copy...), voi syy olla esimerkiksi jokin seuraavista:

- Kiintolevyn/CD-ROM:in ohjaintyyppi on väärä
- Kiintolevy ei ole kunnossa
- Kiintolevyn/CD-ROM:in SCSI-terminointi ei ole oikein.

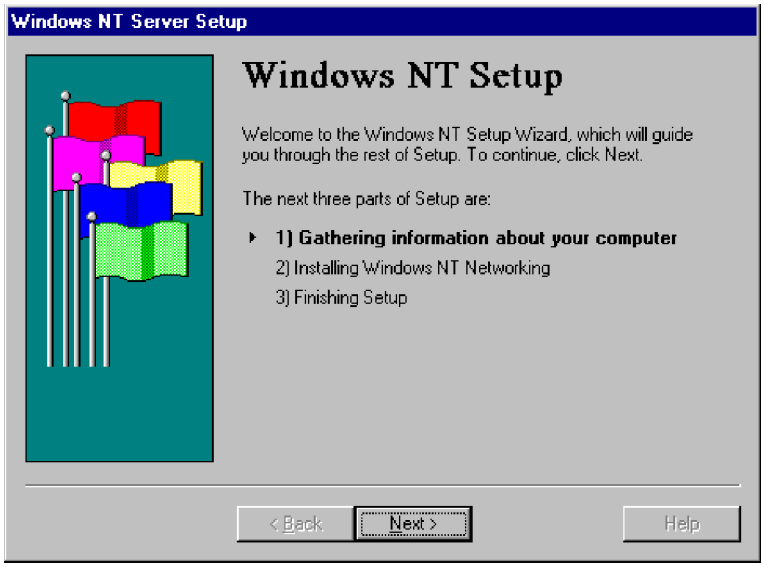
Kun saat ilmoituksen uudelleenkäynnistyksestä, poista levyke ja Windows NT 4.0 Serverin asennus-CD-ROM CD-ROM-asemasta ja paina **ENTER**. Uudelleenkäynnistyksen jälkeen asennus jatkuu graafisella (Windows-) osuudella.



Poista ehdottomasti levykkeet levykeasemasta ja myös CD-levyt CD-ROM-asemasta, koska uudelleenkäynnistyksessä saatat muuten saada NT:n virheilmoituksia!

Ns. buuttaavia CD-ROM-asemia käytettäessä yleinen virhe on se, että CD-ROM-asemaan on unohdettu NT:n asennus-CD-ROM, ja NT:n käynnistystiedostot yritetään ladata CD-ROM:ilta.

13) Näyttöön tulee **Windows NT Setup**.



Kerätään tietoja tietokoneesta - **Gathering information about your computer** - paina **Next**

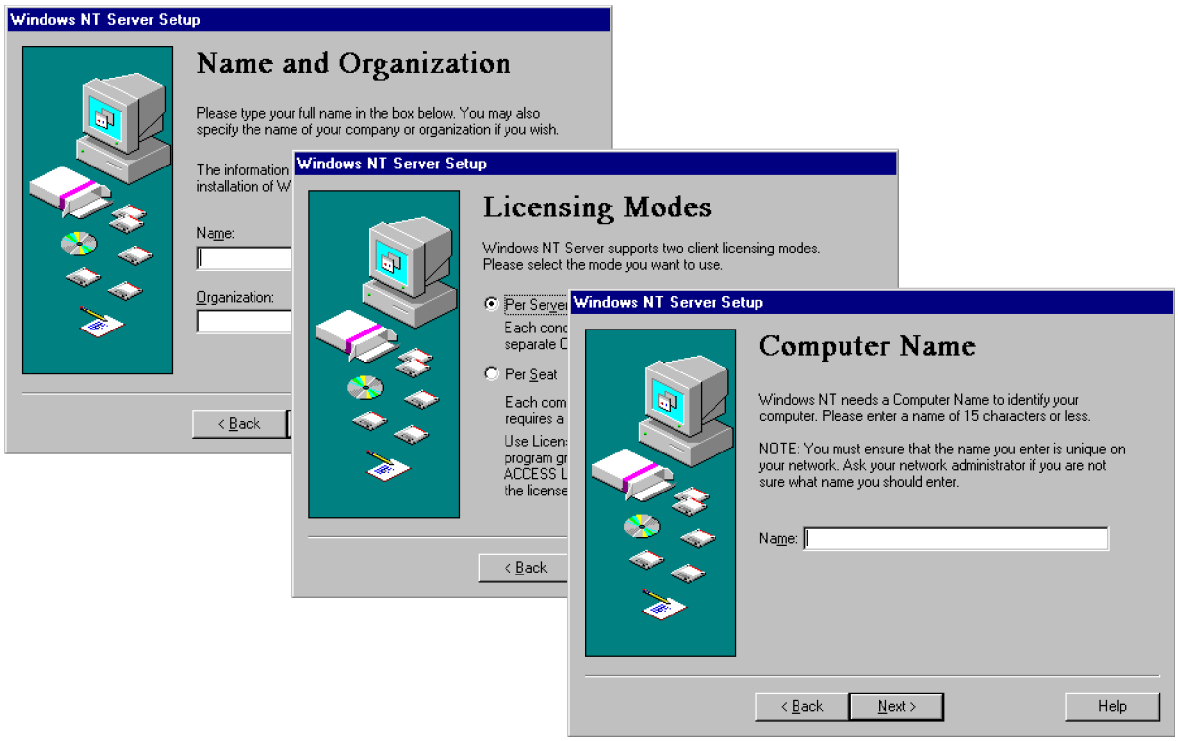
14) Kirjoita seuraavat tiedot:

- Nimi (**Name**) - Lisenssinhaltijan nimi
- Yritys (**Company**) - Yrityksen/organisaation nimi (ei pakollinen), paina **Next**
- Anna **CD Key,** paina **Next**

Seuraavaksi annettava lisenssiasetukset:

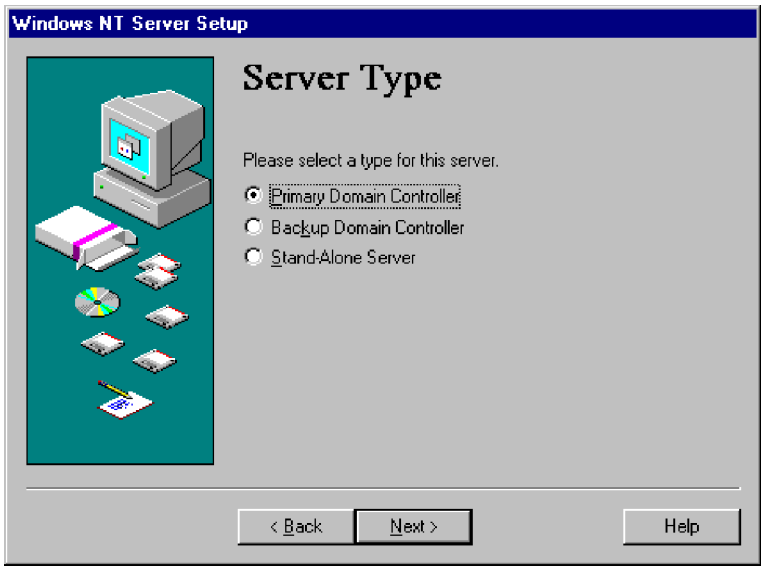
- **Per Server** - koskee tiettyä **samanaikaista käyttäjämäärää**. Anna käyttäjämäärä ruutuun **Per Server for:**
- **Per Seat** - kyseessä on rajoittamaton käyttämäärä. Käytä valvontatyökalujen **License Manager**-ohjelmaa asettaaksesi käyttäjät.

Asetuksia voit myöhemmin muuttaa **kerran Ohjauspaneelin** (Control Panel) **Licensing** -kuvakkeella siten, että **Per Server** voidaan muuttaa **Per Seat**-tyyppiseksi. Tällöin työasemassa tulee olla lisenssiasiat kunnossa. Paina **Next**



Anna seuraavaksi **palvelimen** nimi (**Computer Name**). Paina **Next**

15) Tämän jälkeen annetaan palvelimen tyyppi eli rooli.



Server Type:

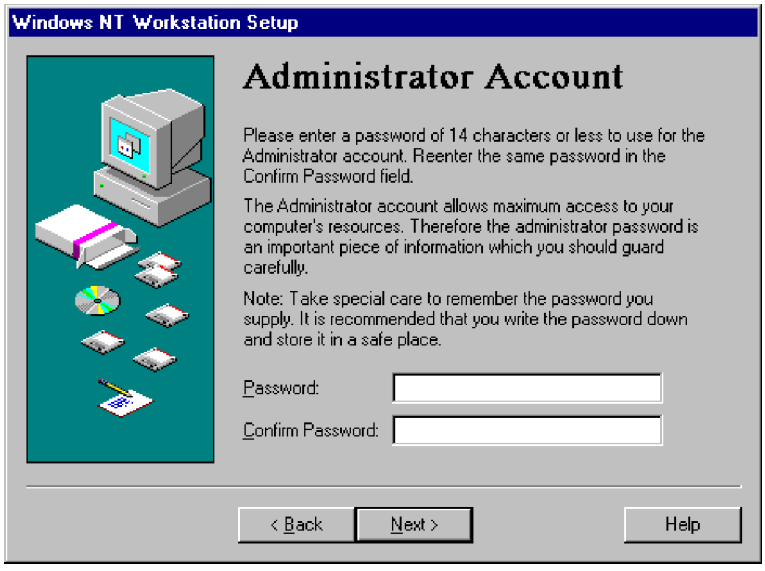
- **Primary Domain Controller** - tämä on oletus. Anna tällöin toimialueen nimi, jonka palvelin perustaa. PDC-palvelimia voi olla vain yksi jokaista toimialuetta kohti!

- **Backup Domain Controller** - toimialueen (*Domain*) varapalvelin; anna tällöin toimialueen nimi, johon palvelin liittyy.

- **Stand-Alone Server** - erillinen palvelin, joka ei mahdollista keskitettyä käyttäjienhallintaa eikä käsittele käyttäjien kirjautumispyyntöjä.

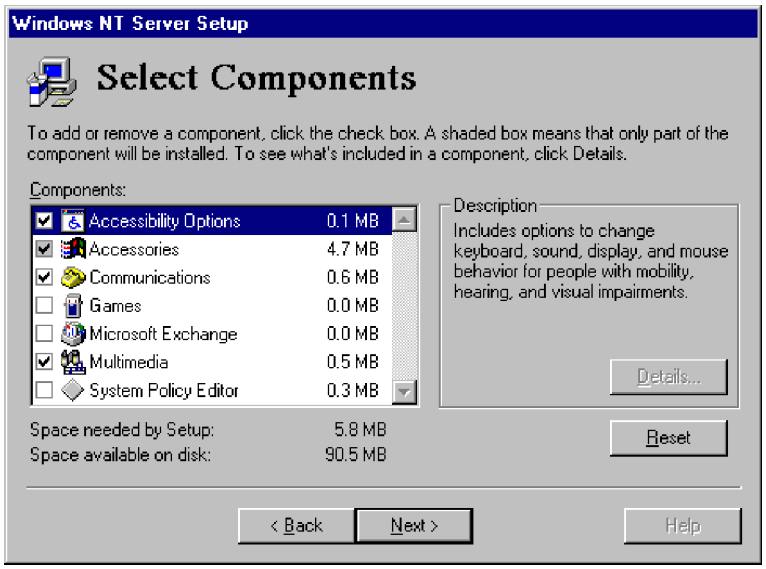
Jos asennat **Primary Domain Controller**- tai **Stand-Alone Server**-tyyppistä palvelinta, anna seuraavaksi **Administrator**-käyttäjätunnuksen salasana kyseisellä toimialueella. Salasana on annettava kahdesti samanlaisena. Jos jätät **Password**-kohdan tyhjäksi, saat siitä varoituksen. Varmista salasanan oikeinkirjoitus **Confirm Password** -kohdassa.

Muista, että NT erottelee isot ja pienet kirjaimet!

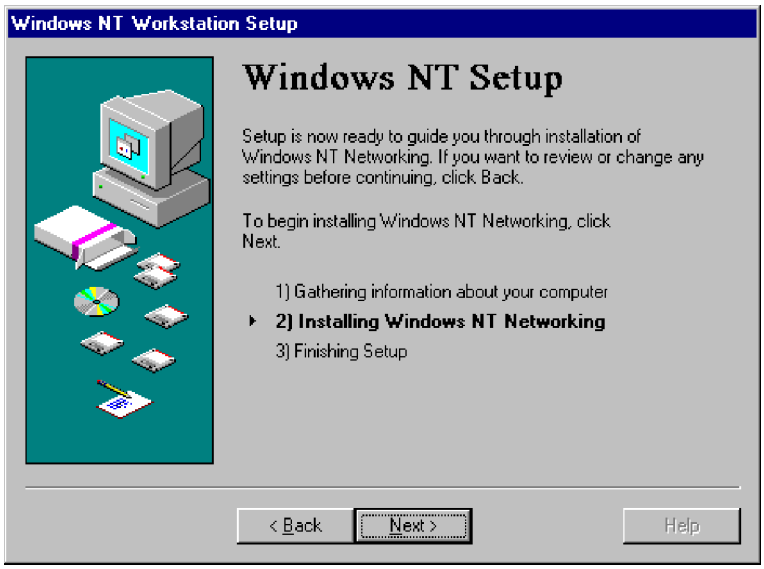


16) Luodaanko korjauslevyke (Repair Disk) - **Kyllä** (Yes) tai **Ei** (No). Kannattaa tehdä. Paina **Next**

17) Seuraavaksi valitaan Windows NT:n asennettavat osat (Select Components) - tee halutut valinnat ja paina **Next**

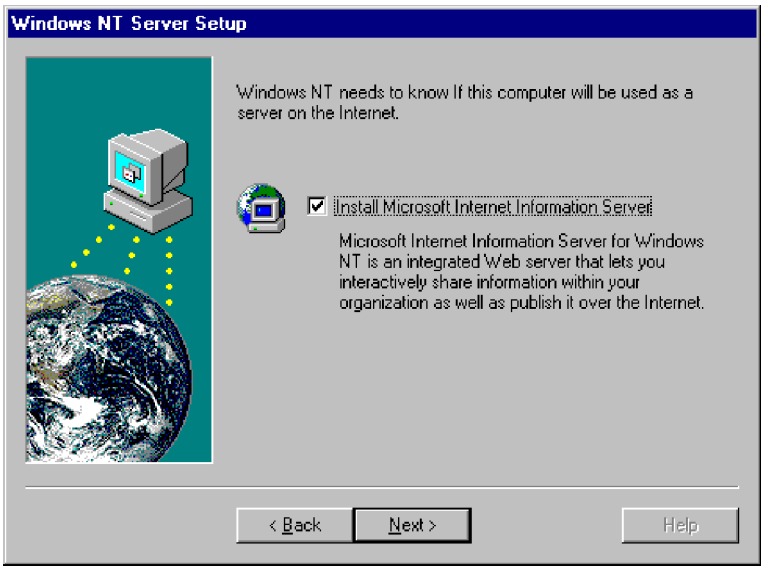


18) Asennetaan verkkotoiminnot. Paina **Next**



19) Voit valita verkkokortin tai ISDN-sovittimen lisäksi (Wired to the network) **etäyhteyden verkkoon** (Remote access to the network). **Wired to the network** on pakollinen valinta. Paina **Next**

20) Seuraavaksi voit valita **Internet Information Server 2.0**:n asennuksen. Jos asennat sen (tämä on tietysti oletus), asenna jäljempänä myös TCP/IP-protokolla



21) Seuraavaksi asennetaan verkkokortti (Network adapter). Paina aloita etsintä (Start Search). Jos kortti löytyi, paina **Next** - muuten voit valita luettelosta **Select from list**

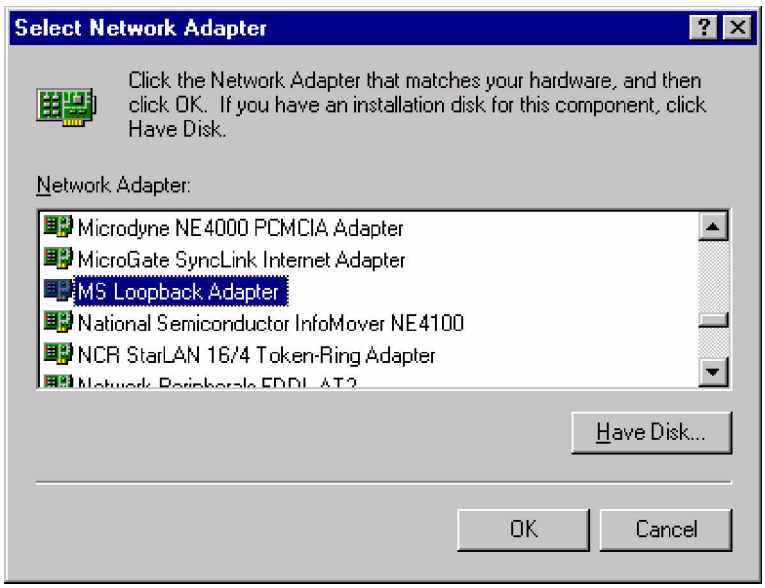
Huomaa:

- Jos kyseessä on ISA-väylän verkkokortti, voit antaa tarvittavat asetukset; esimerkiksi **I/O Port Address**, **Interrupt Number**, **Transceiver Type** (10 Base T, Thin Net (BNC, COAX), Thick Net (AUI/DIX)). Tavallinen virhe on se, että verkkokortti määritellään käyttämään eri liitäntää kuin mihin verkkokaapeli on liitetty

- Saatat saada ilmoituksen **The current netcard parameters are not verified correct and may result in usage problems or system failure. Use them anyway?** Tämä voi johtua ohjelmallisesti asennettavan verkkokortin käyttämistä muista, aiemmin annetuista asetuksista ja verkkokortti mahdollisesti kuitenkin toimii

- Jos verkkokortti on asennettava manuaalisesti jumppereilla tai DIP-kytkimillä, saatat kohdata vaikeuksia - asennus saattaa esimerkiksi jumiutua jossakin vaiheessa. Voithan kokeilla, mitä tapahtuu - jos asennus jumiutuu, tarkista kortin asetukset ja valitse seuraavalla asennuskerralla **oikeat** asetukset. Apunasi voit käyttää **NT Hardware Query Tool**-apuohjelmaa.

- Jos et pysty asentamaan haluamaasi verkkokorttia, asenna **MS Loopback Adapter**. Tällöin ehkä pystyt suorittamaan asennuksen loppuun saakka (tai ainakin hieman eteenpäin...). Toinen vaihtoehto on asentaa tietoliikennesovitin etäkäyttöyhteyttä varten (esimerkiksi modeemi, ISDN-sovitin jne).



22) Valitse protokollat - oletuksena ovat **TCP/IP** (se tarvitaan jos asennat **Internet Information Serverin**) ja **NWLink IPX/SPX Compatible Transport**. Voit lisätä muitakin tarpeen mukaan, mutta *älä lisää turhia protokollia*. Jos et käytä Novell-palvelimia, voit jättää asentamatta **NW Link IPX/SPX Compatible Transportin**.

NetBEUI Protocol-protokollaan ei liity asennusvaiheessa mitään erityisiä asetuksia. Protokolla ei kuitenkaan ole ns. reitittävä protokolla, eli se ei toimi reititinverkoissa.

Jos asennat **Backup Domain Controller** (BDC) -tyyppistä palvelinta, valitsemillasi protokollilla on **ehdottomasti** päästävä kiinni **Primary Domain Controller** (PDC) -palvelimeen. TCP/IP-protokollalla tarvitaan reititinverkossa **LMHOSTS**-tiedosto, jossa on PDC:n tiedot: esimerkiksi

123.123.123.123 serveri1 #PRE #DOM:hallinto

Paina **Next**.

23) Valitse asennettavat palvelut (**Network Services**) - oletukset käyvät tavallisesti mainiosti. Paina **Next**.

24) Tämän jälkeen asennetaan verkon komponentit. Jos valitsit TCP/IP:n, tulee kysymys **DHCP-palvelimen** käytöstä. Jos haluat IP-osoitteen DHCP-palvelimelta, valitse kyllä (**Yes**). Palvelimissa tulisi

yleensä olla kiinteä IP-osoite eli tavallisesti on syytä vastata ei (**No**). Tällöin voit määritellä TCP/IP-asetukset (katso tarkemmin tästä kirjasta **luvusta 7**). Paina **Next**.

25) Seuraavaksi voit määritellä **sidokset** (**Bindings**) eri verkkopalveluille - oletukset käyvät tavallisesti mainiosti. Paina **Next**.

26) Seuraavaksi asennusohjelma **käynnistää verkon** (ready to start the network). Paina **Next**.

Jos asennat **Backup Domain Controller**-tyyppistä palvelinta, anna seuraavaksi toimialueen nimi (**Domain**) ja jonkun **järjestelmänvalvojatason** (**Administrator Name**) käyttäjätunnus sekä sen salasana (**Administrator Password**) kyseisellä toimialueella.

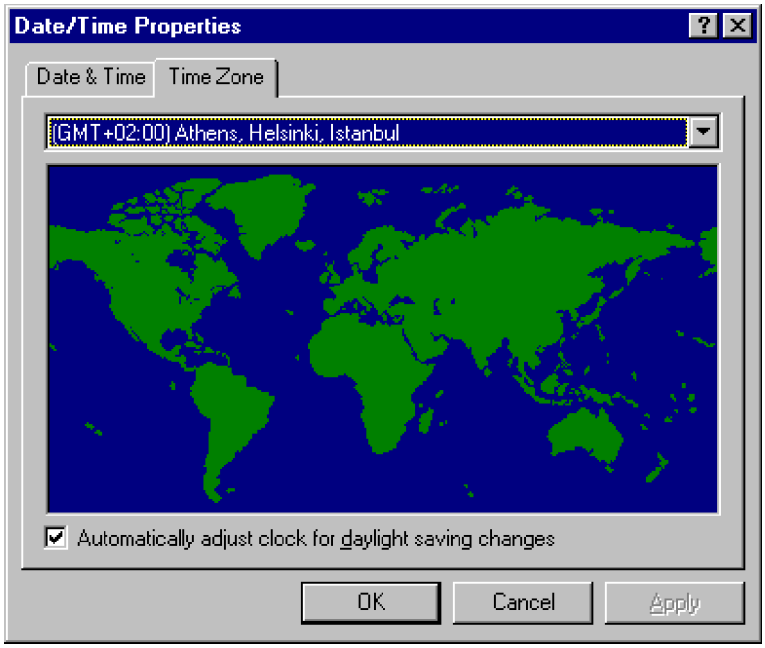
Huomaa:

- Reititinverkossa on syytä käyttää TCP/IP-protokollaa ja tehdä esim. levykkeelle LMHOSTS-tiedosto, jossa on määritelty kyseisen toimialueen PDC:n nimi ja IP-osoite

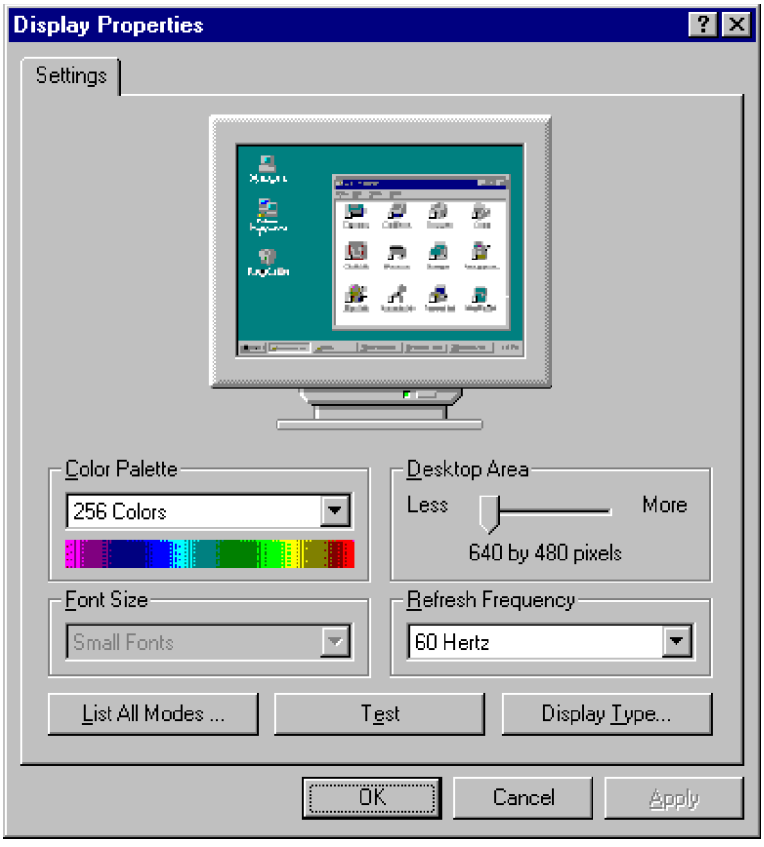
- Muista, että NT erottelee isot ja pienet kirjaimet salasanoissa!

27) Lopetetaan asennuksen tämä vaihe - paina **Finish**. Jos valitsit **Internet Information Serverin** asennettavaksi, anna tarvittavat asetukset. Katso tarvittaessa ohjeita **luvusta 9**.

28) Anna **päivämäärän ja ajan ominaisuudet** (Date/Time Properties), valitse oikea aikavyöhyke ja mahdollinen kesä/talviaikaan siirtyminen. Paina **sulje** (Close)



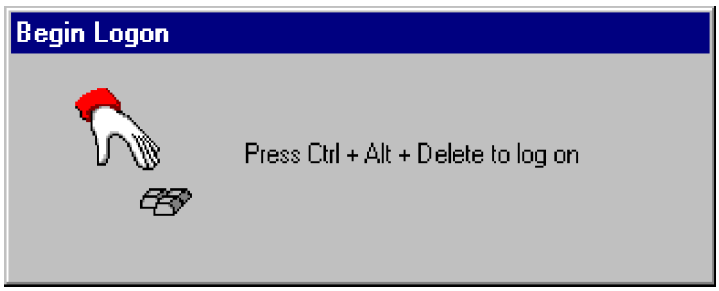
29) Asenna näyttö; kun olet antanut haluamasi asetukset, paina **testi** (**Test**) ja **OK**. Vastaa kysymykseen näkyikö testikuva ja paina **OK**



30) Tee tarvittaessa korjauslevyke (**Emergency Repair Disk**). Jos asennat Backup Domain Controlleria, kestää hetken, kun käyttäjätietokanta kopioidaan Primary Domain Controllerista. Valitse lopuksi **tietokoneen uudelleen käynnistys** (**Restart computer**).

Seuraavassa käynnistyksessä tehdään mahdollinen konversio FAT-tiedostojärjestelmästä NTFS-tiedostojärjestelmään, jos olet valinnut konversion tehtäväksi.

31) Kirjaudu **Järjestelmänvalvoja** (Administrator) -tunnuksella käyttäjäksi



Tee tarvittaessa ensimmäiset asennuksen jälkeiset asetukset:

- Tarkista **Ohjauspaneelista** (Control Panel) **Maa-asetukset** (International)
- Luo tarvittaessa luottosuhteet verkkoalueiden välille
- Luo käyttäjätunnukset ja verkkojaot
- Asenna muut palvelut (**DHCP**, **WINS**, **DNS, RAS**, **Mail**)
- Jos kiintolevylle on jäänyt väliaikainen asennushakemisto, esimerkiksi **WIN_NT.~LS**, voit poistaa sen
- Muista nauhavarmistukset ja korjauslevykkeen päivittäminen!

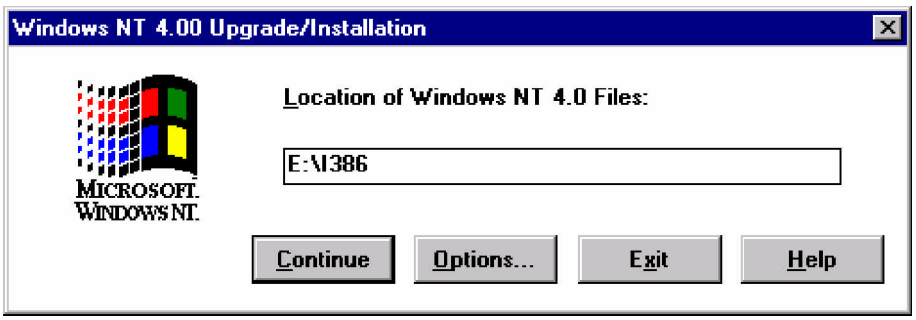
Windows NT 3.51:n päivitys

Jos mikroon on aiemmin asennettu Windows NT 3.5x, voit asennuksen yhteydessä valita **päivityksen** (*Upgrade*) Windows NT 4.0-versioon.

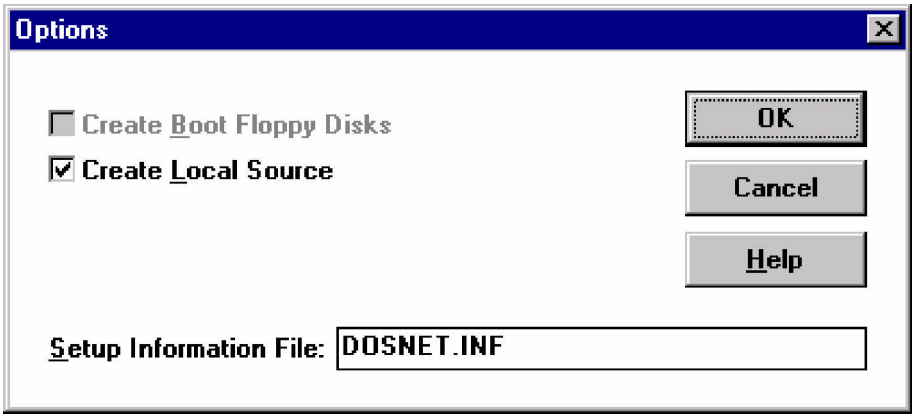
Voit suorittaa versiopäivityksen Windows NT 3.51:stä versioon 4.0 myös Windows NT 4.0:n asennushakemistosta (esimerkiksi **i386**) komennolla **WINNT32**. Menetelmää tarvitaan automaattisessa asennuksessa, jolloin päivitys suoritetaan esimerkiksi komennolla **WINNT32 /U:C:\USERS\DEFAULT \UPGRADE.TXT /S:I:\I386 /B**, joka etsii asennusta ohjaavaa skriptiä **c:\users\default** -hakemistosta.

Jos asennat Windows NT 4.0 -CD-ROM:in asemaan, ja käyttöjärjestelmäversiosi tukee CD-ROM:in automaattista käynnistystä, voit päivittää tai asentaa Windows NT 4.0:n suoraan CD-ROM:in päävalikosta .

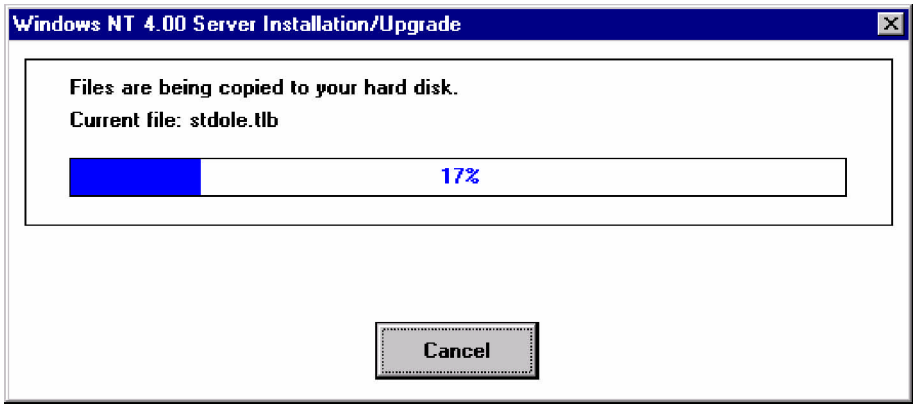
1) Valitse **Windows NT Asennus** (Install Windows NT).



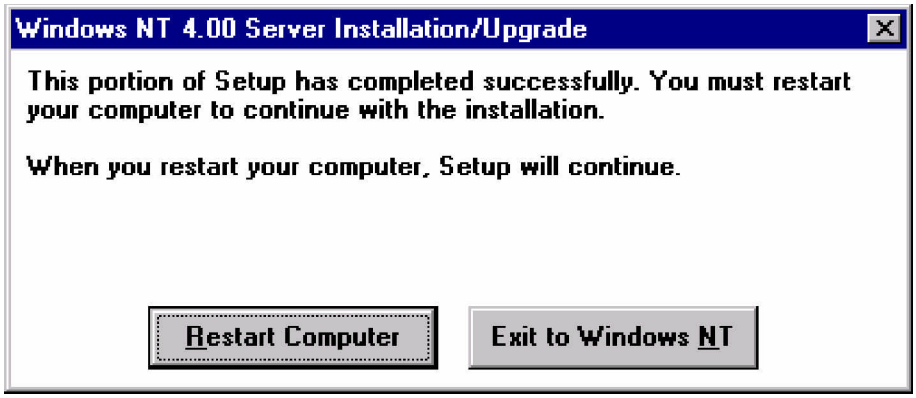
Voit valita **Options** - lähinnä luodaanko paikallinen asennushakemisto (Local Source) sekä asetusta ohjaavan INF-tiedoston nimen (oletuksena **DOSNET.INF**)



2) Jos valitsit paikallisen asennushakemiston luomisen, painamalla **OK** se luodaan. Voit keskeyttää asennuksen painamalla **Cancel**.



3) Lopuksi voit **Käynnistää tietokoneen** (Restart Computer) uudelleen. Tämän jälkeen asennus jatkuu normaalisti.



Automaattinen asennus

Windows NT 4.0:n kopioiminen mikrosta toiseen toimivana on äärimmäisen hankalaa, mutta Windows NT 4.0:n (työaseman tai palvelimen) voi asentaa automaattisesti useillakin eri menetelmillä. Automaattinen asennus tarkoittaa menetelmää, jossa asennuksessa tarvittavat tiedot on annettu tavalla tai toisella jo etukäteen, ja itse asennus sujuu enemmän tai vähemmän automaattisesti.

Eri vaihtoehtoja ovat ainakin:

- **Microsoft Systems Management Server** - tällä voit hoitaa NT:n asennuksen automaattisesi käyttäjän kirjautumisen yhteydessä, tai tyypillisesti luoda asennusta ohjaavan työn (*job*). Jos SMS on sinulle tuttu, tiedät millaisesta työmäärästä on kysymys. Jos SMS ei ole sinulle entuudestaan tuttu, niin siinä ajassa kun opettelet sen sujuvan käytön, olet jo asentanut joitakin satoja NT-työasemia

- **OEM-hakemisto** alihakemistoineen - NT:tä asennettaessa viitataan näihin hakemistoihin. Esimerkiksi MS Officen asentaminen C:-asemaan tehtäisiin viittaamalla **OEM\C\MSOffice**-hakemistoon

- **SYSDIFF** - ensin asennetaan mallityöasema ja ajetaan **SYSDIFF**. Sitten asennetaan sovellukset ja muutoksista luodaan SYSDIF-Fin avulla *snapshot* komennolla **SYSDIFF /DIFF**. Näihin muutoksiin viitataan OEM-hakemistossa

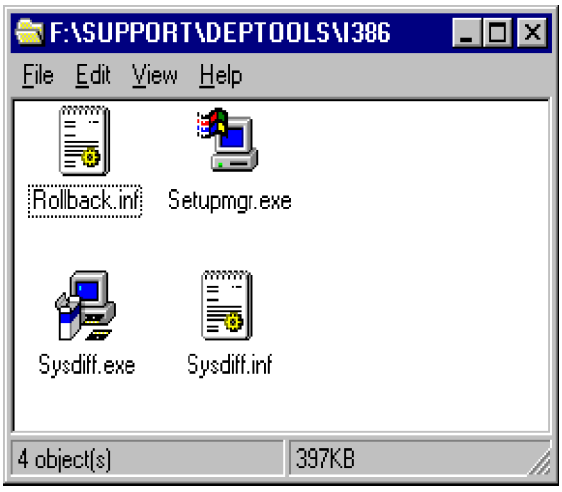
- **Vastaustiedostot** (Answer file), näihin tekstipohjaisiin asennusta ohjaaviin tiedostoihin viitataan WINNT:n valitsimella **/U**
- **Uniqueness Database File** (UDF) on laajennus vastaustiedostoihin
- **Setupmgr** - tällä voi tehdä vastaustiedostoja, ja käyttö on suhteellisen selväpiirteistä.

Oma mielipiteeni on, että palvelimet - varsinkin PDC:t - tulisi asentaa aina perinteisellä menetelmällä paikalliselta CD-ROM:ilta ilman automaattista asennusta, jotta voidaan varmistua asennuksen onnistumisesta.

Työasemien ja vaikkapa BDC:ien asennus voidaan hoitaa vastaustiedostoilla (Answer file). Sysdiff ja OEM-menetelmät soveltuvat mielestäni OEM-laitekauppiaiden esiasennuksiin.

Windows NT 4.0:n CD-ROM:in hakemistossa **Support\Deptools** on kaksi asennusta helpottavaa apuohjelmaa, **Sysdiff** ja **Setupmgr**. Sysdiffin avulla voit määritellä useiden työasemien asennuksissa kaikkien työasemien yhteiset asetukset.

Olepa varovainen hakemistosta **mahdollisesti** löytyvän **Rollback**-ohjelman kanssa! Se on tarkoitettu OEM-laitevalmistajien käyttöön ja osaamaton Rollback-ohjelman käyttö voi sotkea koko NT-järjestelmän! Ohjelma löytyy **9.8.1996** valmistetuilta CD-ROM:eilta, mutta ei enää **14.10.1996** valmistetuilta CD-ROM:eilta:



Setup Managerin (Setupmgr) avulla voit tehdä asennuskriptejä. Windows NT:n voi asentaa automaattisesti, ilman asennusvaiheen kysymyksiä asennushakemistosta jne. Tällöin tarvitset ns. **vastaustiedoston** (*Answer File*). Yleisesti käytetään myös termiä **asennusskripti**. WINNT-komento

tuntee valitsimen **/U:**, jonka perään annetaan käytetyn asennuskriptin nimi.

Automaattinen asennus etenee seuraavin vaihein:

1) Tee uusi vastaustiedosto tai muokkaa vanhaa

2) Tallenna se

3) Suorita asennus **WINNT**- tai **WINNT32**-komennolla.

Asennuksen vaiheet

Varsinaisessa asennuksessa tee seuraavat toimenpiteet:

1) Asenna tai kopioi työaseman/palvelimen CD-ROM:in prosessorin mukainen asennushakemisto verkkoon joko CD-ROM-asemaan tai kiintolevyn hakemistoon; esimerkiksi **i386** - kiintolevyn on oltava alustettu FAT-tyyppiseksi ennen asennusta!

2) Jaa e.m. hakemisto tai CD-ROM verkkoon

3) Kopioi vastaustiedosto jaettuun hakemistoon esimerkiksi työaseman/palvelimen mukaisella nimellä, esimerkiksi **WS12.TXT**

4) Uusi asennus tehdään komennolla **WINNT** ja vanhan asennuksen päivitys komennolla **WINNT32**. Valitsimet ovat:

WINNT /U:W:\WS12.TXT /S:X:\ /B

Tällöin käytetään W:-aseman juurihakemistossa olevaa skriptiä ja asennetaan **X:**-asemasta. **/B** asentaa käynnistystiedostot kiintolevylle, jolloin käynnistyslevykkeitä ei tarvita.

Päivitys suoritettaisiin komennolla:

WINNT32 /U:W:\WS12.TXT /S:I:\I386 /B

joka etsii skriptiä **W:**\-hakemistosta. Asennuksessa käytetään **I:**-aseman **i386-hakemistoa** - tässäkin **/B** asentaa käynnistystiedostot kiintolevylle, jolloin käynnistyslevykkeitä ei tarvita.

Päivitys ilman vastaustiedostoa (käyttämällä aiemmin annettuja asetuksia toimivassa, päivitettävässä NT-järjestelmässä) tehtäisiin siis:

```
WINNT32 /U
```

5) Asennuksen aikana asennuslevykkeitä ei siis tarvita. Asennustiedostot kopioidaan mikron kiintolevylle **WIN_NT.~LS** -nimiseen väliaikaiseen hakemistoon. Jos vastaustiedostossa ei ole vastausta, käyttäjältä pyydetään haluttu valinta tai asetus.

Vinkkejä:

- Verkkokäynnistyslevykkeen (Network Boot Disk) voit tehdä NT-palvelimen **Network Client Administrator**-ohjelmalla
- Kiintolevyn asennetaavassa mikrossa on oltava alustettu FAT-tyyppiseksi ennen asennusta
- Muun hakemiston/kiintolevyn asennustiedostojen väliaikaishakemistolle voit antaa valitsimella **/T:** esimerkiksi **E:**-aseman käyttö:

```
X:\WINNT /U:C:\UNATTEND.TXT /T:E /S:X:\
```

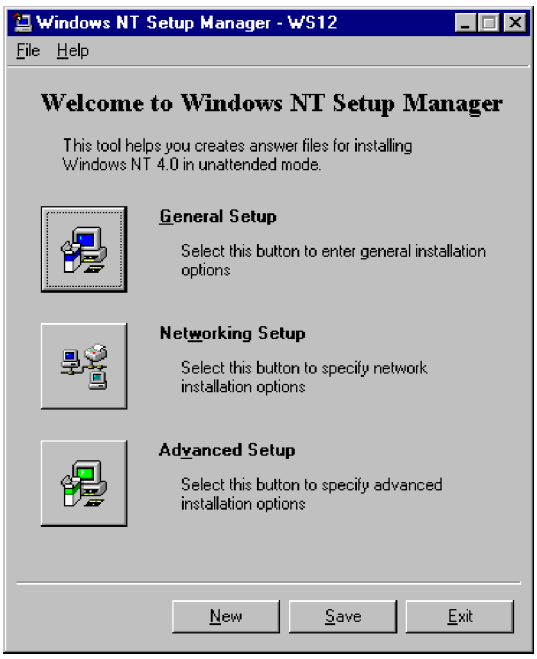
- Jos asennus jymähtää, syynä voi olla se, että asennusohjelma ei löytänyt SCSI-ohjainta tai asensi väärän SCSI-laiteohjaimen.

Vastaustiedoston luominen

Vastaustiedosto voidaan tehdä seuraavasti:

- Muokkaamalla Windows NT:n asennus-CD-ROM:in i386-hakemistosta löytyvää **UNATTEND.TXT**-tiedostoa. Tämä on hankalampi menetelmä - helpompi on seuraava menetelmä

- Windows NT 4.0 Serverin ja Windows NT 4.0 Workstationin CD-ROM:illa tulevalla **Windows NT Setup Manager**illa - hakemistossa **Support\Deptools. Setupmgr-ohjelmaa ei tarvitse erikseen asentaa**



Vastaustiedostossa tulee määritellä seuraavat asiat:

- Windows NT:n asennushakemisto
- Onko kyseessä päivitys vai uusi asennus
- Käyttäjätunnus (ei päivityksessä komennolla WINNT32)
- Organisaation nimi (ei päivityksessä komennolla WINNT32)
- Työaseman/palvelimen nimi (ei päivityksessä komennolla WINNT32)
- Tuote-ID
- Työaseman/palvelimen rooli (ei päivityksessä komennolla WINNT32)
- Työryhmän/toimialueen nimi (ei päivityksessä komennolla WINNT32)
- Aikavyöhyke

- Verkkokortti asetuksineen ja protokollat (ei päivityksessä komennolla WINNT32).

Luotuasi sopivat asetukset tallenna vastaustiedosto valinnalla **File | Save as**.

Esimerkki vastaustiedostosta

Esimerkiksi halutaan tehdä vastaustiedosto seuraavanlaiselle palvelimelle (samalla periaatteella voidaan asentaa myös työasema):

- Käyttäjätunnus on **R.Brunkkeberg**
- Organisaatio on **FishWare Finland Oy**
- Palvelimen nimi on **V3**
- Tuote-ID 1923894-43434-54
- Ei varmisteta laitteistokokoonpanoa asennuksen yhteydessä
- Palvelimen tyyppi **Backup Domain Controller**
- Kuuluu toimialueelle **VERSTAS**
- Windows NT:n asennus **oletushakemistoon**
- Varmuuden vuoksi halutaan kuitata laitteistoasetukset (ei välttämättä työasemien asennuksissa, mutta toki palvelimessa hyvä tarkistaa)
- Näytön asetukset varmuuden vuoksi perus-VGA:lle
- Aikavyöhyke on Suomen (**GMT +2**)
- Lisenssimenetelmä **Per Seat**
- Käyttää Compaq 32-Bit NetFlex/NetFlex-2-korttia

- **TCP/IP**-protokollan asetukset: **IP-osoite** 130.9.63.9, **aliverkko** 255.255.0.0, **yhdyskäytävä** 130.9.63.1, **DNS-palvelimet** 130.9.63.3, 130.9.63.5 ja 130.9.63.10, **WINS-palvelimet** 130.9.63.5 ja 130.9.63.10, **DNS-nimi** V3.VERSTAS.FI

- Asennetaan **etäkäyttöpalvelu** (Remote Access Service, RAS) COM1:een modeemiyhteydelle (sekä sisään- että ulossoitto), TCP/IP-protokollatuki koko verkkoon siten että etäkäyttäjä saa DHCP-palvelimelta osoitteen, modeemi on Boca Modem V.Fast Class

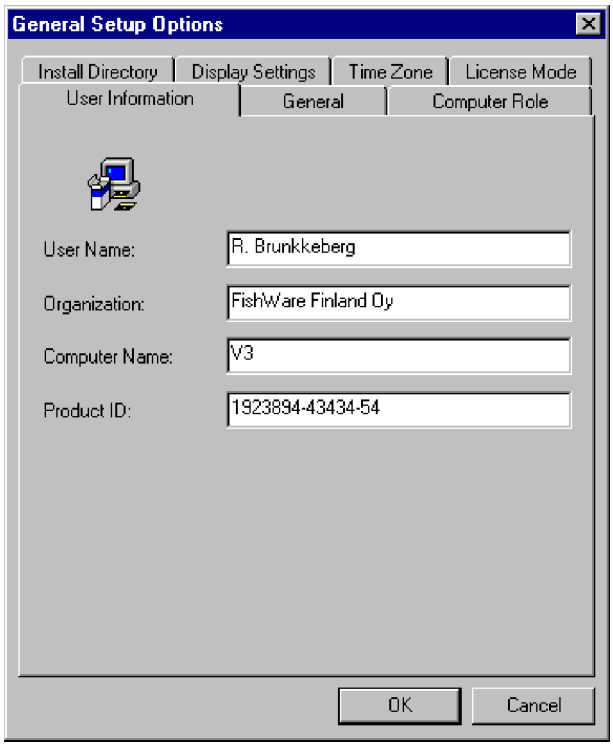
- Asennetaan **Internet Information Server** (IIS) WWW-hallintaohjelmineen

- Asennetaan suomalainen näppäimistö

- Tiedostojärjestelmä konvertoidaan NTFS-tyyppiseksi.

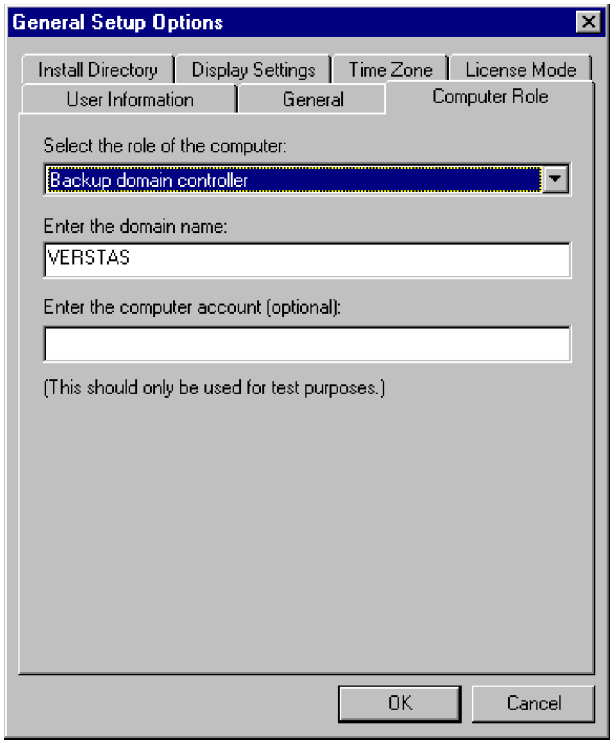
Vastaustiedosto luodaan painamalla ensin **General Setup** ja antamalla yleiset asetukset:

- Anna **User Information**-välilehdessä käyttäjätunnus, organisaatio, palvelimen nimi ja Tuote-ID



- **General**-välilehdessä valitaan laitteistoasetusten varmistus asennuksen yhteydessä valinnalla **Confirm Hardware During Setup**

- **Computer Role**-välilehdessä palvelimen tai työaseman tyyppi (esimerkissä **Backup Domain Controller**) ja toimialueen nimi (esimerkissä **VERSTAS**)



- **Install Directory** -välilehdessä oletushakemiston (**Use Default Directory**) käyttäminen

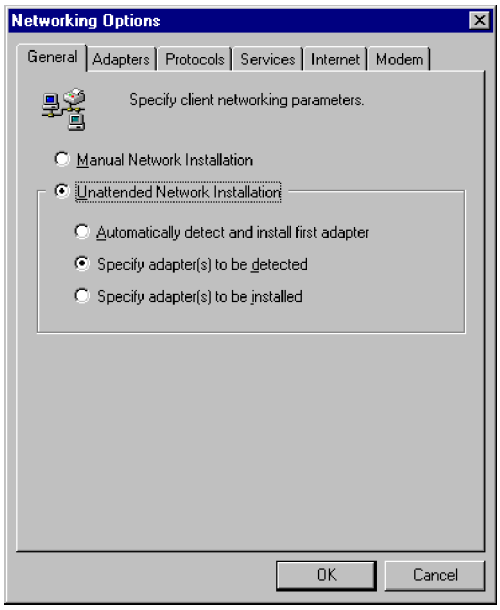
- **Display Settings**-välilehdessä perus-VGA:n käyttäminen

- **Time Zone**-välilehdessä aikavyöhyke

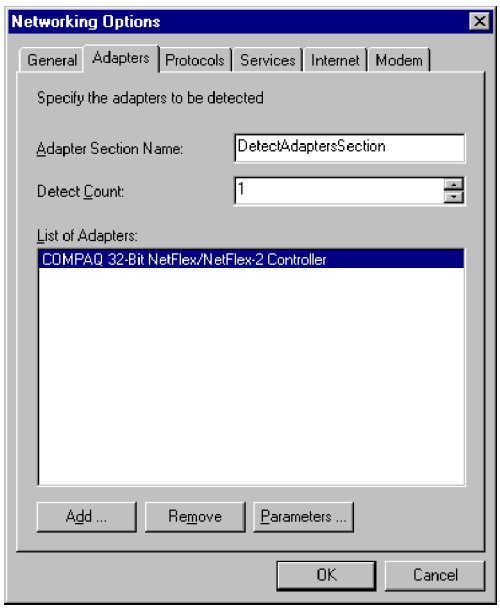
- **License Mode**-välilehdessä sovellettava lisenssimenetelmä.

Paina **Networking Setup** ja anna verkon asetukset:

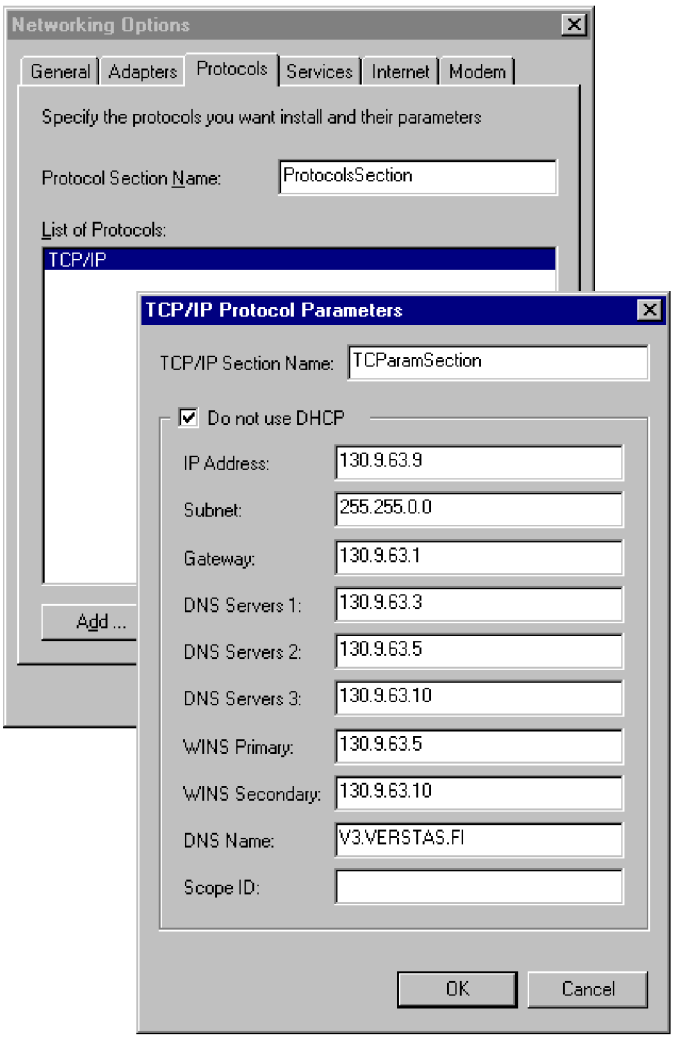
- Valitse **General**-välilehdessä joko manuaalinen (**Manual**) tai automaattinen (**Unattended**) verkkoasetusten asentaminen. Unattended-menetelmällä voit asentaa tuen automaattisesti asennusohjelman tunnistamalle verkkokortille, tai kuten tässä esimerkissä, tunnistettava kortti määritellään.



- Koska **General**-välilehdessä valittiin tunnistettava kortti, **Adapters**-välilehdessä voit määritellä verkkokortin; tässä esimerkissä on kyseessä Compaq 32-Bit NetFlex/NetFlex-2. **Detect Count** kertoo montako kyseistä korttia mikrossa on

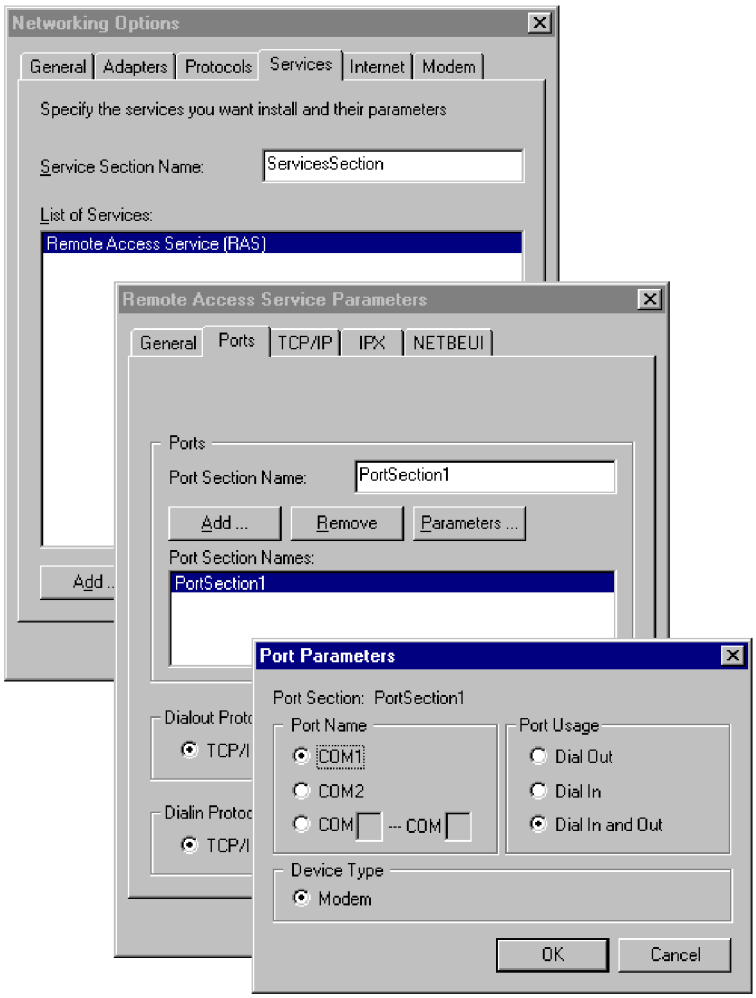


- **Protocols**-välilehdessä valitaan protokolla asetuksineen, tässä ei käytetä DHCP:tä, vaan asetukset annetaan erikseen:

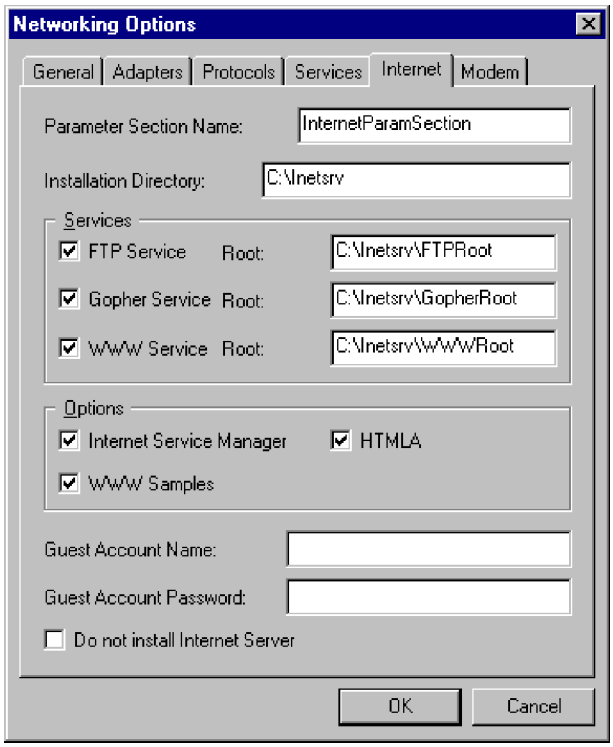


- **IP-osoite** 130.9.63.9, **aliverkko** 255.255.0.0, **yhdyskäytävä** 130.9.63.1, **DNS-palvelimet** 130.9.63.3, 130.9.63.5 ja 130.9.63.10, **WINS-palvelimet** 130.9.63.5 ja 130.9.63.10, **DNS-nimi** V3.VERSTAS.FI

- **Services**-välilehdessä valitaan verkkopalvelut (SNMP, RAS, Netware) asetuksineen. Painamalla **Parameters** voidaan määrittää palvelun konfigurointi. Tässä esimerkissä COM1:ssä on modeemi, siten että sen kautta sallitaan sekä tulevat että lähtevät soitot.



- **Internet**-välilehdellä asetetaan Internet Information Serverin asetukset. Sen voi myös jättää asentamatta valitsemalla **Do not install Internet Server**. **HTMLA** mahdollistaa Internet Information Serverin hallinnan Internet-selaimella.



- **Modem**-välilehdellä voit määritellä asennettavan modeemin asetukset.

Advanced Setup -painikkeella voit antaa lisäasetuksia:

- **General**-välilehdessä voit ottaa käyttöön suomalaisen näppäimistön

- **File System** -välilehdessä voit määritellä konversion NTFS-tiedostojärjestelmään (Convert to NTFS).

Luotuasi sopivat asetukset tallenna vastaustiedosto valinnalla **File | Save as**.

Luodun asetustiedoston keskeiset edellämainitut asetukset:

[Unattended] - yleiset asetukset
FileSystem = ConvertNTFS
ConfirmHardware = yes
TargetPath = *
KeyboardLayout = "Finnish"

[UserData] - lisenssitiedot ja mikron nimi
FullName = "R. Brunkkeberg"
OrgName = "FishWare Finland Oy"
ComputerName = V3
ProductId = "1923894-43434-54"

[GuiUnattended] - aikavyöhyke
TimeZone = "(GMT+02:00) Athens, Helsinki, Istanbul"

[LicenseFilePrintData] - sovellettava lisenssimenetelmä
AutoMode = PerSeat

[Display] - näytön asetukset
BitsPerPel = 8
XResolution = 640
YResolution = 480
VRefresh = 60
AutoConfirm = 1

[Modem] - modeemin asentaminen
InstallModem = ModemParameters

[ModemParameters] - modeemin asetukset
COM1 = "Boca Modem V.Fast Class"

[Network] - verkon asetukset
DetectAdapters = DetectAdaptersSection
InstallProtocols = ProtocolsSection
InstallServices = ServicesSection
InstallInternetServer = InternetParamSection
InstallDC = VERSTAS

[DetectAdaptersSection] - verkkokortti
LimitTo = NETFLX
NETFLX = NETFLXParamSection

[ProtocolsSection] - protokollien asetukset
TC = TCParamSection

[TCParamSection] - TPC/IP-asetukset
DHCP = no
IPAddress = 130.9.63.9
Subnet = 255.255.0.0
Gateway = 130.9.63.1
DNSServer = 130.9.63.3, 130.9.63.5, 130.9.63.10
WINSPrimary = 130.9.63.5
WINSSecondary = 130.9.63.10
DNSName = V3.VERSTAS.FI

[ServicesSection] - asennettavat palvelut
RAS = RASParamSection

[RASParamSection] - RAS-asetukset
PortSections = PortSection1
DialoutProtocols = TCP/IP
DialinProtocols = TCP/IP
NetBEUIClientAccess = Network
TcpIpClientAccess = Network
UseDHCP = YES
ClientsCanRequestIPAddress = NO
IpxClientAccess = Network
AutomaticNetworkNumbers = YES
AssignSameNetworkNumber = YES
ClientsCanRequestIpxNodeNumber = NO

[PortSection1] - käytettävä sarjaportti
PortName = COM1
DeviceType = Modem
PortUsage = DialInOut

[InternetParamSection] - IIS:n asetukset
InstallDir = C:\Inetsrv
InstallINETSTP = 1
InstallWWW = 1
WWWRoot = C:\Inetsrv\WWWRoot
InstallGOPHER = 1
GopherRoot = C:\Inetsrv\GopherRoot
InstallFTP = 1
FTPRoot = C:\Inetsrv\FTPRoot
InstallADMIN = 1
InstallW3SAMP = 1
InstallHTMLA = 1

Hakemistorakenne ja jaetut resurssit

Asennuksen jälkeen NT-työaseman ja -palvelimen hakemistorakenne on seuraavanlainen, jos käytetään oletusasetuksia (asennetaan C:-asemaan ja WINNT-hakemistoon):

Päähakemistotaso:

TEMP	**Hakemisto väliaikaistiedostoille**
WINNT	NT:n järjestelmähakemistojen juuri; jaettu verkkoon nimellä **ADMIN$**

Edellisen alla ovat seuraavat hakemistot:

CONFIG	Rekisteritietokannan tiedostot
CURSORS	Kohdistimet
FONTS	Fontit, piilotettu hakemisto
HELP	Opasteet
INF	Asetustiedostot
MEDIA	Multimediatiedostot
PROFILES	Käyttäjien profiilit
SHELLNEW	Käynnistystiedostot muutamalle sovellukselle
REPAIR	Kopio korjauslevykeestä
SYSTEM	True Type -fontteja ja Windows 3.1-sovellusten DLL:t
SYSTEM32	NT:n apuohjelmat ja hallintasovellukset

Edellisen alla ovat seuraavat hakemistot:

DHCP	DHCP-palvelun tietokannat (vain palvelimessa)

DRIVERS	Laiteohjaimet eli ajurit
OS2	OS/2-alijärjestelmä (DLL:t jne)
RAS	Etäkäyttötyöaseman ja -palvelimen **MODEM.INF** jne
REPL	Monistuspalvelun hakemistot; **EXPORT** vienti, **IMPORT** tuonti
SPOOL	Laiteohjaimet kirjoittimille; jos kirjoitin on jaettu verkkoon, myös alihakemisto **DRIVERS** on jaettu verkkoon. Tällöin NT-mikrot ottaessaan jaetun kirjoittimen käyttöönsä saavat samalla tarvittavat kirjoittimen laiteohjaimet
WINS	WINS-palvelun tietokannat (vain palvelimessa)

Huomattavaa:

- **DRIVERS**-hakemiston alla on **ETC**, jossa on TCP/IP:n isäntätiedostoja (mm. **LMHOSTS.SAM**, jota voi käyttää pohjana **LMHOSTS**-tiedostoa luotaessa)

- **REPL**-hakemiston alla on **IMPORT\SCRIPTS**, jossa ovat käyttäjien kirjautumiskomentojonot (Logon Script). Se on jaettu verkkoon nimellä **NETLOGON kaikissa Windows NT-ohjauskoneissa** (*Domain Controller*). Jakoa ei pidä poistaa!

- Jos kirjoitin on jaettu verkkoon, myös hakemisto **WINNT\SYSTEM32\SPOOL\DRIVERS** on jaettu verkkoon nimellä **print$**. Tällöin NT-mikrot ottaessaan jaetun kirjoittimen käyttöönsä saavat samalla tarvittavat kirjoittimen laiteohjaimet

- Kaikki loogiset kiintolevyt on jaettu verkkoon nimellä **<levyasematunnus>$**, esimerkiksi **C$, jonka Verkonvalvojat (Administrators)** voivat ottaa käyttöönsä

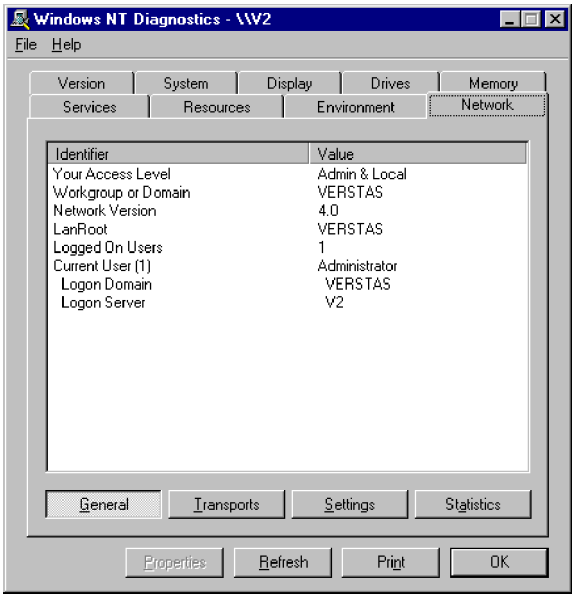
- **IPC$** liittyy nimettyihin putkiin, joiden avulla mm. prosessit kommunikoivat. Jakoa ei pidä poistaa!

Asennuksen jälkeen

Seuraavassa luettelo eräistä toimenpiteistä, joita kirjoittaja on nähnyt hyödyllisiksi NT:n asentamisen jälkeen.

Tarvitset Administrator-tason oikeudet useimpiin asetuksiin. Toiminnot eivät välttämättä ole kriittisyysjärjestyksessä, ja niitä voi vapaasti soveltaa käyttöympäristön ja -tilanteen mukaan. Lisää vinkkejä vastaanotetaan!

- Kokeile kirjautuminen toimialueelle Administrator-tason tunnuksella. Windows NT Diagnostiikkaohjelmalla näet yhteenvedon kirjauksesta



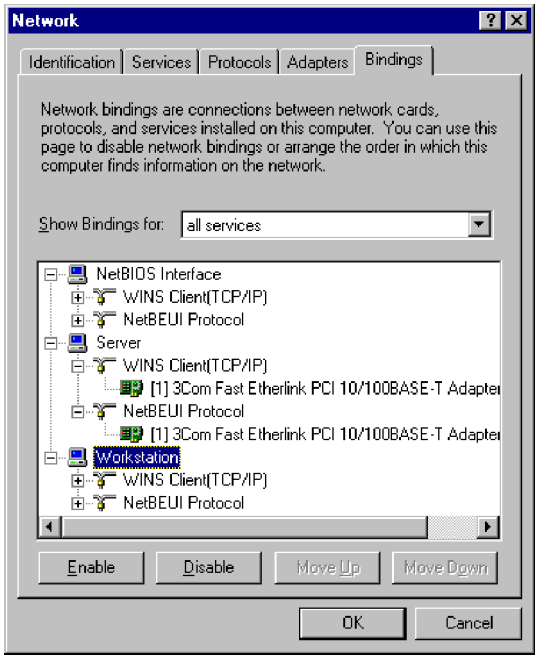
- Tarkista verkon toiminta vaikka **NET VIEW-komennolla** tai **Network Neighborhoodilla**. Jos näet vain kyseisen työaseman/palvelimen (vaikka verkossa muutakin saattaa olla), tarkista seuraavat asiat:

  - Tapahtumanvalvonta **Event Viewer** punaisten **Stop**-virheilmoitusten varalta

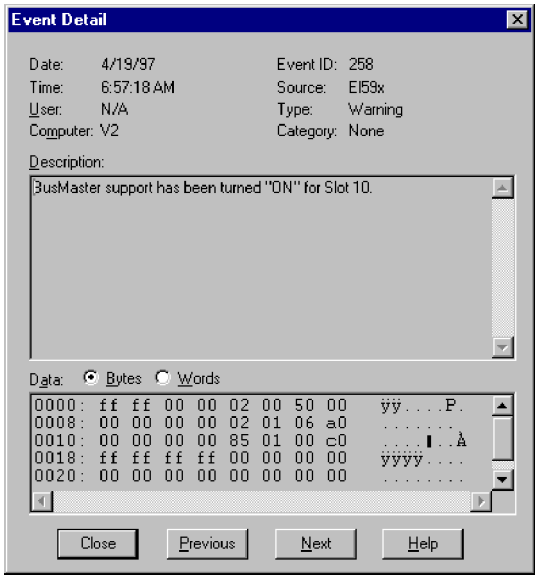
  - **Verkkokortin tyyppi** ja **asetukset** (IRQ, I/O Address, jne) sekä ennen kaikkea oikea **verkkoliitäntä** (10 Base T/parikaapeli, Thin Net/BNC/koaksiaalikaapeli, Thick Net/AUI/DIX)! Löytyvät **Ohjauspaneelista** (Control Panel) **Verkko** (Network) -kuvakkeen avulla. EISA-väylän mikrossa asetukset saattavat olla muutettavissa EISA-väylän asetusten

kautta

- Protokollat
- Sidokset.

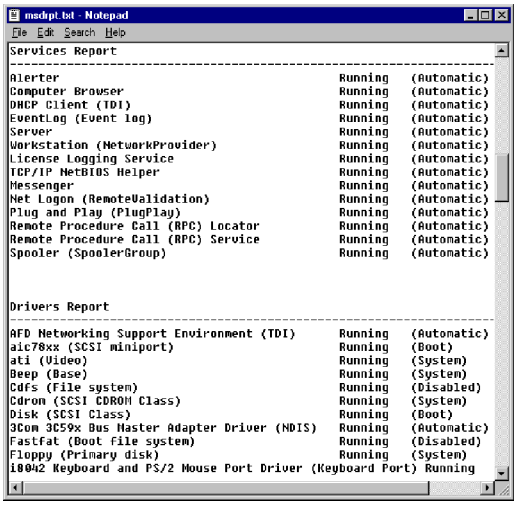


■ Tarkista tapahtumanvalvonnalla **Event Viewer** käynnistymisen tapahtumat. Selauspalvelun (**Browser**) ilmoitukset (**Type: Information**) eivät ole vaarallisia mutta väärin konfiguroidun oheislaitteen saattavat olla!

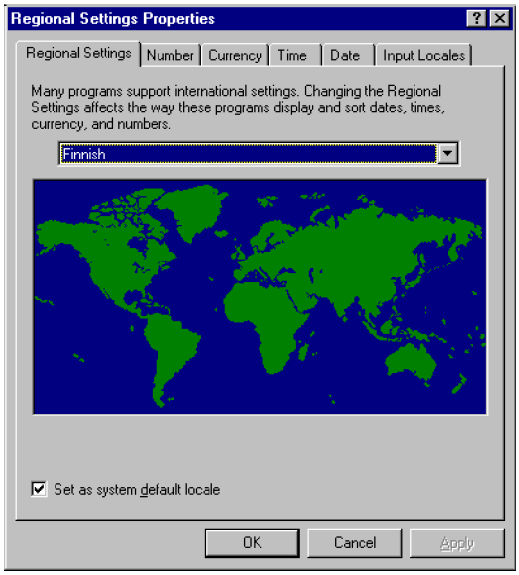


- Asenna tarvittaessa uusin **Service Pack**; komento on **UPDATE** a.o. Service Pack:in hakemistossa. Uusimman asentaminen riittää! Asenna myös tarvittaessa ns. **HotFix**it

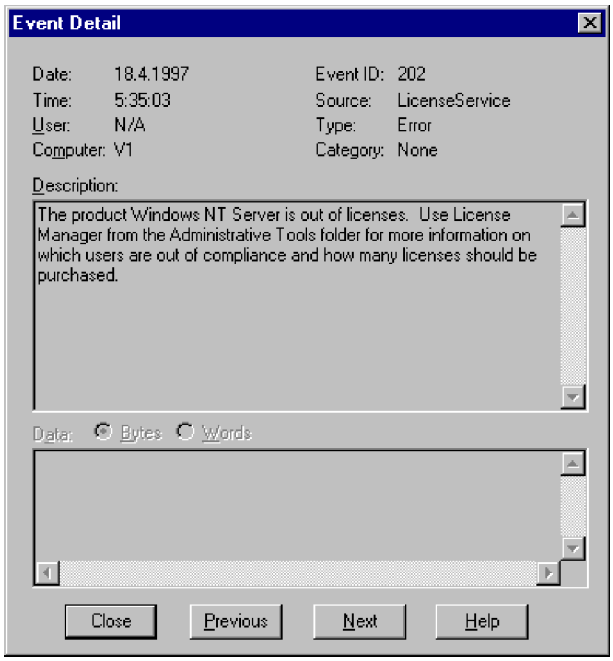
- Raportin asetuksista voi Windows NT Diagnostiikkaohjelmalla tulostaa tiedostoon valinnalla **File** | **Save Report**. Tiedostoa voi tutkia esimerkiksi **Muistiolla** (Notepad)



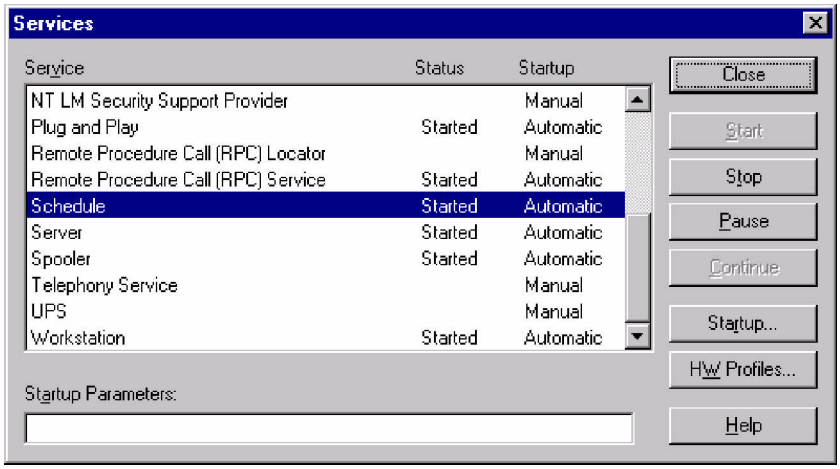
- Tarkista **Ohjauspaneelista** maakohtaiset asetukset **Regional Settings**: suomalaiset asetukset ovat muuten yleensä OK, mutta pitkä päiväyksen muoto voi olla englanninkielisessä NT:ssä esimerkiksi *Januaryta* (vrt. Tammikuuta). Tarkista samalla **Input Locales**-välilehdestä kielen asetuksista näppäimistön asetuksiksi suomalainen (**Keyboard Layout: Finnish**). Voit asettaa antamasi asetukset kaikille palvelimen paikallisille käyttäjille käyttöön **Set as system default locale**-valinnalla



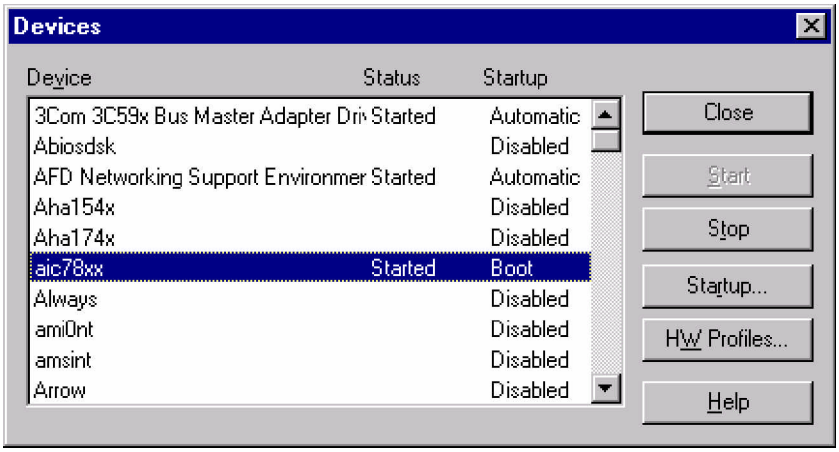
- Tarkista palvelimessa lisenssiasetukset **License Managerilla** sekä lisenssien ylitykset tapahtumanvalvonnalla **Event Viewer**



- Tarkista, että palvelimessa toimivat **tarpeelliset palvelut** (**Services**): tarpeellisia palveluita ovat **Net Logon**, **Server** ja **Workstation**. Jos haluat ajastaa komentoja, myös **Schedule**:n on syytä toimia - se ei oletuksena käynnisty automaattisesti. Voit ajastaa minkä tahansa komentojonon tai komennon (vaikkapa virustorjunnan tai varmistuksen)



- Tarkista laitteiden tila **Devices**; ainakin verkkokortin ja massamuistiohjainten tulisi olla käynnistettyjä

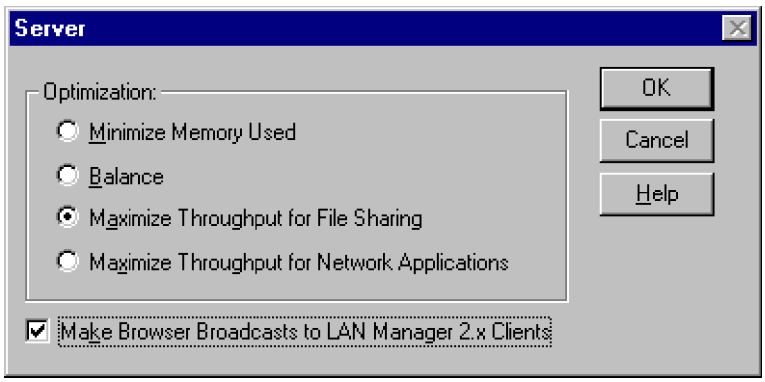


- Komennolla **NET CONFIG SERVER** voit asettaa palvelimen palvelinpalvelun lisäasetuksia, mm. aikakatkaisun; esimerkiksi komennolla

  NET CONFIG SERVER /AUTODISCONNET:-1

  aikakatkaisu otetaan pois käytöstä. Aikakatkaisu on oletuksena 15 minuuttia ja se saattaa joskus aiheuttaa ongelmia

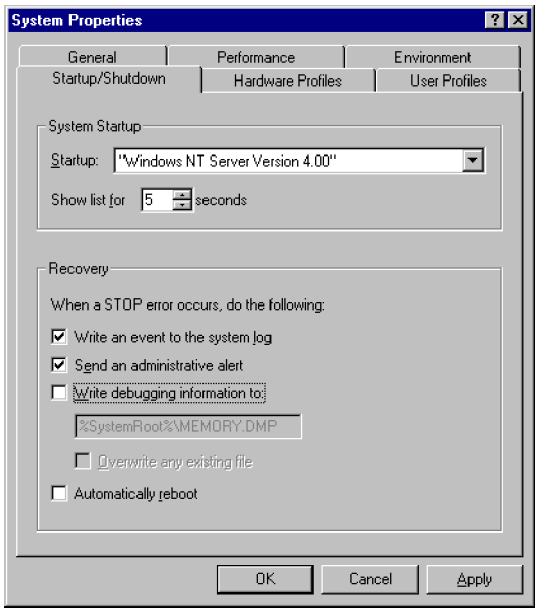
- Tarkista palvelinpalvelun ajoitus: on asetettavissa vain palvelimessa Ohjauspaneelista **Network**-kuvakkeen avulla konfiguroimalla **Server**-palvelua. Jos LAN Manager-työasemat eivät löydä NT-palvelinta verkosta, aseta päälle selaajapalvelun **Computer Browser** yleislähetykset (*Browser Broadcasts*)



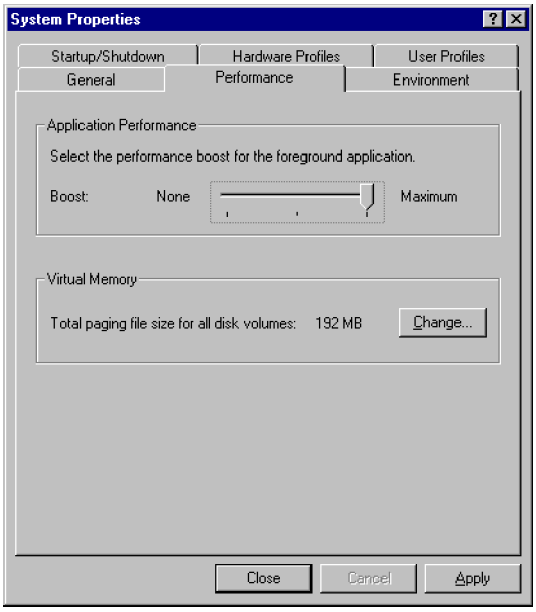
- Tarkista TCP/IP:n asetukset komennolla **IPCONFIG /ALL**. Käytä tarvittaessa **PING**-komentoa tutkiaksesi verkkoyhteyksien toimivuus. Tarkista solmun tyyppi, **DNS:n** ja **LMHOSTS**-tiedoston sekä WINS:in ja DHCP:n käyttö.

```
C:\WINNT> IPCONFIG /ALL

Windows NT IP Configuration

        Host Name . . . . . . . . . . . . . . : v1.verstas.fi
        DNS Servers . . . . . . . . . . . .  : 130.9.63.5
        Node Type . . . . . . . . . . . . . . : Hybrid
        NetBIOS Scope ID. . . . . . . . . . :
        IP Routing Enabled  . . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . . : No
        NetBIOS Resolution Uses DNS : No

Ethernet adapter El59x1:

        Description . . . . . . . . . . . . . . . : Fast Ethernet Adapter
        Physical Address. . . . . . . . . . . . . : 00-20-AF-EA-3C-20
        DHCP Enabled. . . . . . . . . . . . . .  : No
        IP Address. . . . . . . . . . . . . . . . : 130.9.63.3
        Subnet Mask . . . . . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . . . . .:130.9.63.1
```

- Myös **palautumisasetukset** (Crash Recovery) -asetukset saattavat aiheuttaa ongelmia: nimittäin jos joku palvelu tai sovellus aiheuttaa heti käynnistyksen yhteydessä STOP-virheen, palvelin käynnistyy aina uudelleen! Tarkista Ohjauspaneelin **System**-asetusten **Startup/Shutdown**-välilehden **Automatically reboot**. Samalla voit määritellä oletuskäyttöjärjestelmän käynnistysasetukset

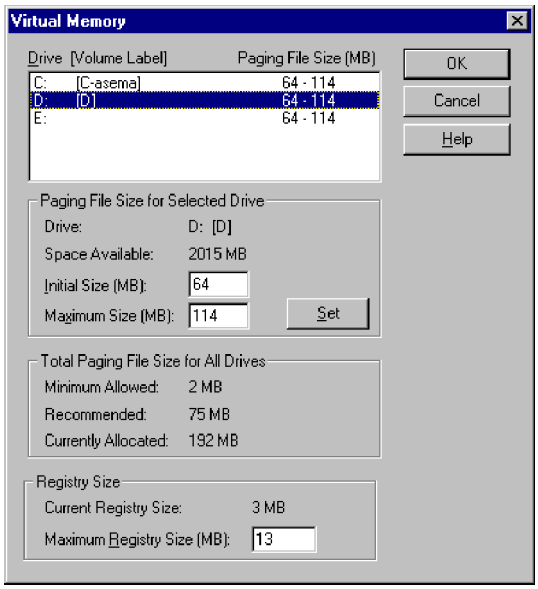


- Tarkista sopiva tehtävien ajoitus Ohjauspaneelista **System**-kuvakkeen **Performance**-välilehden **Application Performance**-asetuksen avulla. Huomaa, että jotkut monitorointiohjelmat saattavat hyydyttää käyttöliittymän, jos **boost** on oikeassa ääriasennossa.

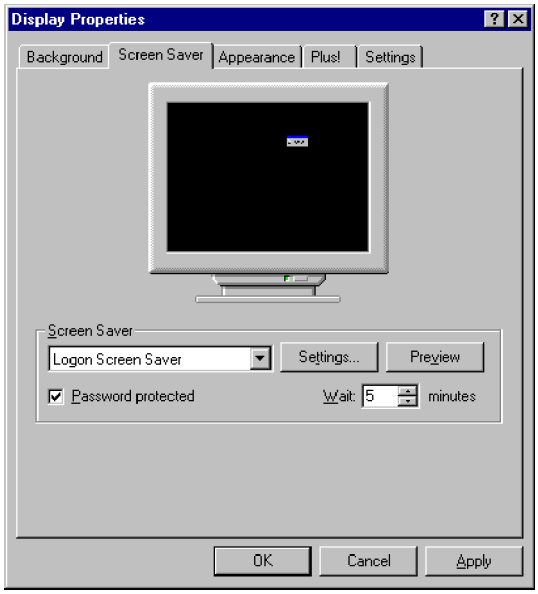


- Sivutustiedoston jakaminen useammalle levylle saattaa nopeuttaa sen käyttöä. Se määritellään Ohjauspaneelista **System**-

kuvakkeen **Performance**-välilehden **Change**-painikkeella. Jos levyosio tulee jostain syystä täyteen (esim. D:-asema), sivutustiedostoa käytetään kuitenkin toiseltakin levyltä



- Näytönsäästäjän salasanasuojaus löytyy työpöydän (**Desktop**) asetuksista. Älä käytä paljon CPU-resursseja nielaisevia (esimerkiksi 3GL) näytönsäästäjiä! **Logon Screen Saver** on kevyimmästä päästä



- Mikron voit lukita nopeimmin painamalla **Ctrl+Alt+Del** ja **ENTER** (Lock Workstation)

- Muista, että NT:n arkkitehtuurista johtuen esimerkiksi käyttöliittymän jumiutuminen ei vielä tarkoita koko palvelimen jumiutumista!

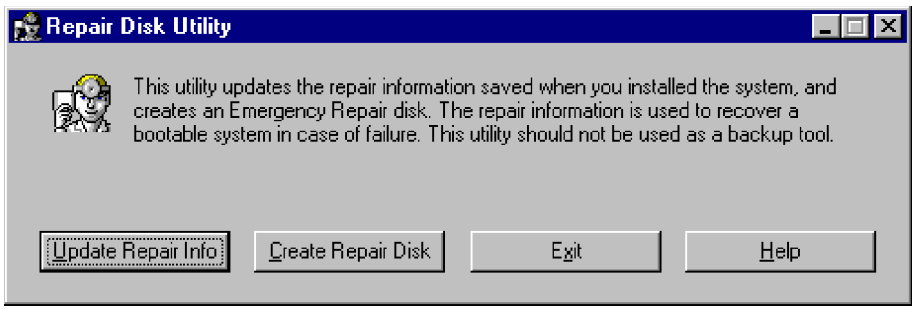
- Komennolla **PENTNT** voi ohittaa ohjelmallisesti vanhemmissa Pentiumeissa viallisen aritmetiikkaprosessorin

- Komennolla **CONVERT** voi muuttaa **FAT**-tiedostojärjestelmän **NTFS**:ksi ilman kiintolevyn osion alustamista

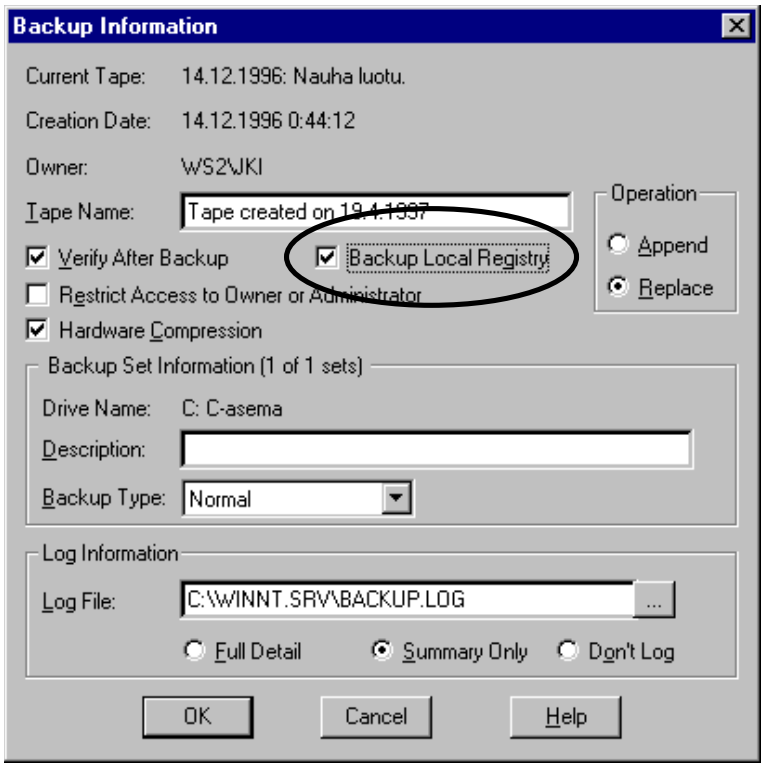
- Tarkista kirjoittimen laiteohjainten saaminen kirjoitinta jakavasta NT-työasemasta/palvelimesta **Event Viewer**-tapahtumanvalvonnalla

- Jos haluat tietyt kuvakkeet oletuskäyttäjälle tai kaikille käyttäjille, käsittele profiilia tarpeen mukaan (**WINNT\Profiles\Default User** ja **WINNT\Profiles\All Users**)

- Muista päivittää laiteasetusten muuttuessa (levyosiot, laiteohjaimet) korjauslevyke **RDISK**-ohjelmalla - esimerkiksi komentoriviltä **RDISK**!



- Testaa nauhavarmistuslaitteen toiminta. Tee koevarmistus ja palautus. Muista varmistaa rekisteri varmistusten yhteydessä!



- Lopuksi: jos kiintolevylle on jäänyt asennusohjelman käyttämä väliaikainen asennushakemisto, esimerkiksi **WIN_NT.~LS**, voit poistaa sen.

Korjauspäivitykset

Seuraavassa käsittelen lyhyesti Windows NT:n **korjausversioiden** eli Service Packien asentamista NT-työasemassa/palvelimessa.

NT:n päivitykset (ja toimintojen laajennukset) ovat nimeltään **Service Pack**. Se on ensinnäkin lokalisoitu eli maakohtainen - englanninkieliseen NT:hen on asennettava englanninkielinen Service Pack ja suomenkieliseen NT:hen on asennettava suomenkielinen Service Pack. Jos asennat englanninkielisen Service Packin suomenkieliseen NT:hen, tiedostojen kieliversiot menevät sekaisin, mutta NT sinänsä toimii. Voi peräti olla, että **Service Pack** ei suostu asentumaan eri kieliseen NT-versioon.

Uusin Windows NT 4.0:n Service Pack on **3** (16.5.1997) ja sen jälkeen on julkaistu kolme korjausta (Hot Fix; tilanne 18.6.1997) . Uudemmissa

Windows NT:n asennus-CD-ROM:eissa jokin Service Packin versio saattaa olla jo mukana, eikä sitä tällöin tarvitse asentaa erikseen.

Tietoja Service Packin ominaisuuksista löydät tavallisesti sen mukana tulevasta HLP- tai README-tiedostosta.

Huomattavaa:

- Päivityksiä voi kysellä jälleenmyyjiltä, etsiä tietokonelehtien yms. BBS-palveluista, Microsoftin FTP-palvelimesta **ftp.microsoft.-com** ja WWW-palvelimesta **www.microsoft.com** sekä TechEd-CD-ROM:ilta

- Eräillä laitevalmistajilla (Hewlett-Packard, Compaq) voi olla omat suosituksensa Service Packien asentamisesta! Esimerkiksi Compaqin tapauksessa on ehkä ensin asennettava NT:n Service Pack ja sitten ennen uudelleenkäynnistystä Compaqin omat ajuriversiot!

- Service Packeista tulee aina ensin englanninkieliset UK-versiot; suomenkieliset FI-versiot tulevat muutamaa kuukautta myöhemmin. Myös tästä syystä palvelimissa usein käytetään UK-versioita

- Service Packit ovat kumulatiivisia eli riittää, että asennat uusimman Service Packin

- Et tarvitse eri Service Packia palvelimeen ja työasemaan. Samassa Service Packissa on mukana molemmat versiot

- Service Packit ovat *lokalisoituja* eli eri kielisissä NT-versioissa tarvitset kyseisen kieliversion Service Packin

- Et voi asentaa esimerkiksi NT 4.0:n Service Packia NT 3.51:een.

Milloin Service Pack tulee asentaa? Tässä oma listani:

- Jos kaikki toimii (varmasti?), niin älä asenna. Jokin sovellus voi kuitenkin vaatia tietyn Service Packin

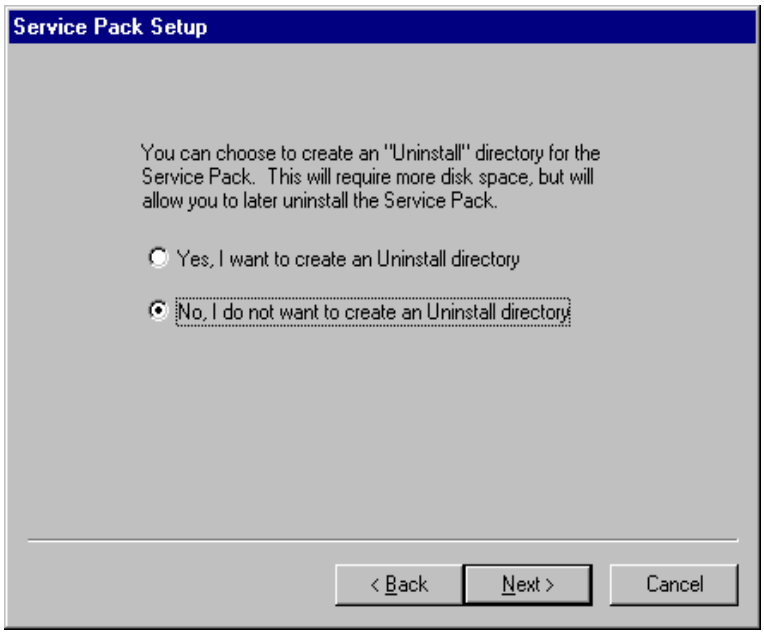
- Tarkista varmuuden vuoksi Service Packin mukana tulevasta HLP- tai README-tiedostosta, josko listalta löytyisi korjauksia suojausongelmiin - suojaukset voivat vuotaa, vaikka *sinä* et siitä olisikaan tietoinen

- Jos NT jymähtelee, luottosuhteet eivät toimi, palvelut lakkaavat toimivasta, massamuistit oikuttelevat, suojaukset vuotavat, TCP/IP-palvelut eivät toimi tai eivät toimi oikein - tarkista tällöin Service Packin mukana tulevasta HLP- tai README-tiedostosta, josko listalta löytyisi korjauksia tuttuihin ongelmiin ja asenna Service Packin

- Samanaikaisesti olisi hyvä päivittää kaikkiin saman toimialueen palvelimiin sama Service Pack.

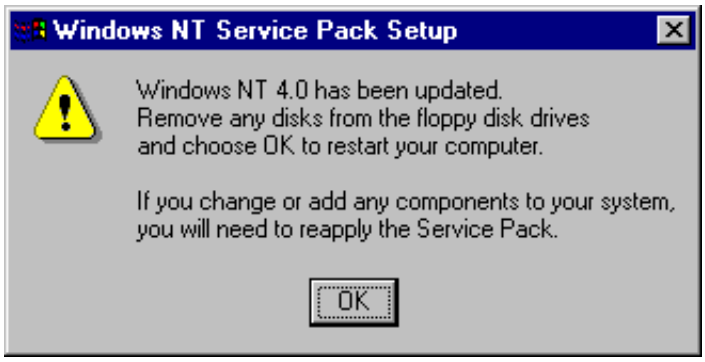
Service Packin asentaminen

Internet-palvelimelta noudettu Service Pack tulee tyyppillisesti yhdessä pakatussa tiedossa. Puretun Service Packin hakemisto saattaa vaatia kymmeniä megatavuja levytilaa. Etsi Service Packin asennushakemisto; asennus tehdään komennolla **UPDATE**.

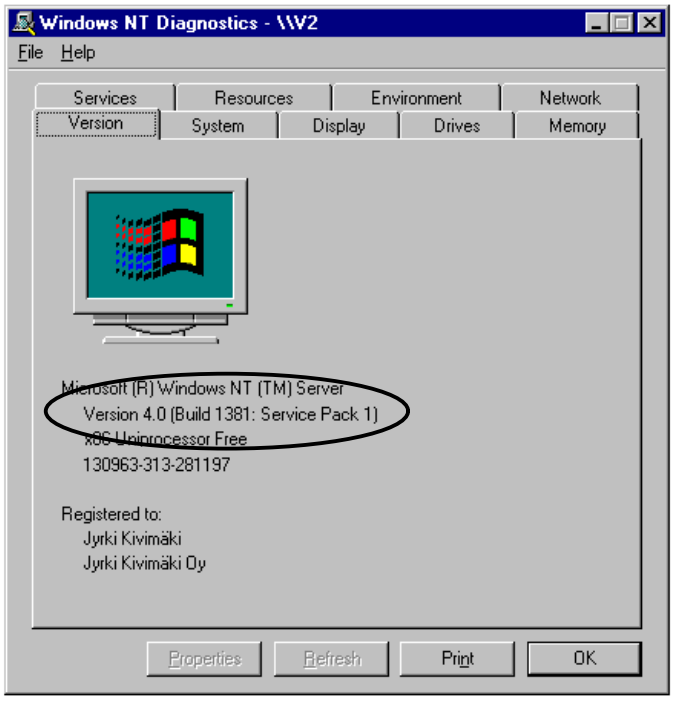


Riippuen Service Packin versiosta voit asennuksen yhteydessä ehkä luoda **Uninstall**-hakemiston, jolloin voit palauttaa tilanteen korjausversiota edeltäneeseen tilaan. Sen voit tehdä myös **UPDATE /U**-komennolla.

Lopuksi mikro tulee käynnistää uudelleen.



Asennetun Service Packin näet mikron käynnistyksessä ja esimerkiksi **Windows NT Diagnostiikalla**.



Windows NT 4.0 Service Pack 2

Windows NT 4.0:n **Service Pack 2** on saanut surullisenkuuluisan maineen. Osa kuuluu ns. kaupunkilaistarinoiden (*Urban Tales*) piiriin, mutta siitä on myös ollut joissakin tapauksissa todellisia ongelmia.

Se korjaa neli- tai useampiprosessorisissa mikroissa esiintyviä jysähdysongelmia sekä korjaa PDC:n ja BDC:n välisiä replikointiongelmia. SP2

sisältää myös uusia API-kutsuja (ReadFileScatter() ja WriteFileGather()), joilla tehostetaan levy-I/O:ta käyttävien sovellusten toimintaa (SQL Server ja Internet Information Server).

Toisaalta se saattaa sotkea NTFS-osioita, jysäyttää koko järjestelmän levykkeelle kirjoitettaessa käytettäessä muistinvaraista virustorjuntaa (McAfee VirusCan, Symantec Norton AntiVirus, Dr Solon AntiVirus ToolKit), jysäyttää NT:n AutoRun-CD-levyjä käytettäessä sekä ehkä mukavin kaikista:

```
Windows NT could not start because the following file is missing or corrupt:

<winnt root>\system32\ntoskrnl.exe

Please reinstall a copy of the above file.
```

Tällöin on etua, jos NT:n järjestelmäosio on FAT-tyyppinen, koska silloin siihen pääsee käsiksi DOS-käynnistyslevykkeellä. Alkuperäiseltä CD-ROM:ilta voi palauttaa kyseisen tiedoston.

Windows NT 4.0 Service Pack 3

Ei-niin-onnistuneen Service Pack **2**:n jälkeen tuli 16.5.1997 jakeluun Service Pack **3**. Kyseessä on ensimmäinen betatestattu Service Pack.

Mukana on:

- CryptoAPI 2.0
- Käyttäjien salasanatietokannan (SAM) tehokkaampi suojaus (128 bit)
- Passfilt.dll tehostamaan salasanoja
- Server Message Block -protokollan tehokkaampi suojaus kirjautumiseen
- Anonyymikäyttäjien oikeuksia rajoitettu - selailua sekä rekisteriin pääsyä rajoitettu

- TCP/IP- ja Telnet -suojaus (Portit 139 ja Telnet -portti)

- Kirjautumisen rajoittaminen niin, että salasanoja ei koskaan lähetetä salakirjoittamattomina.

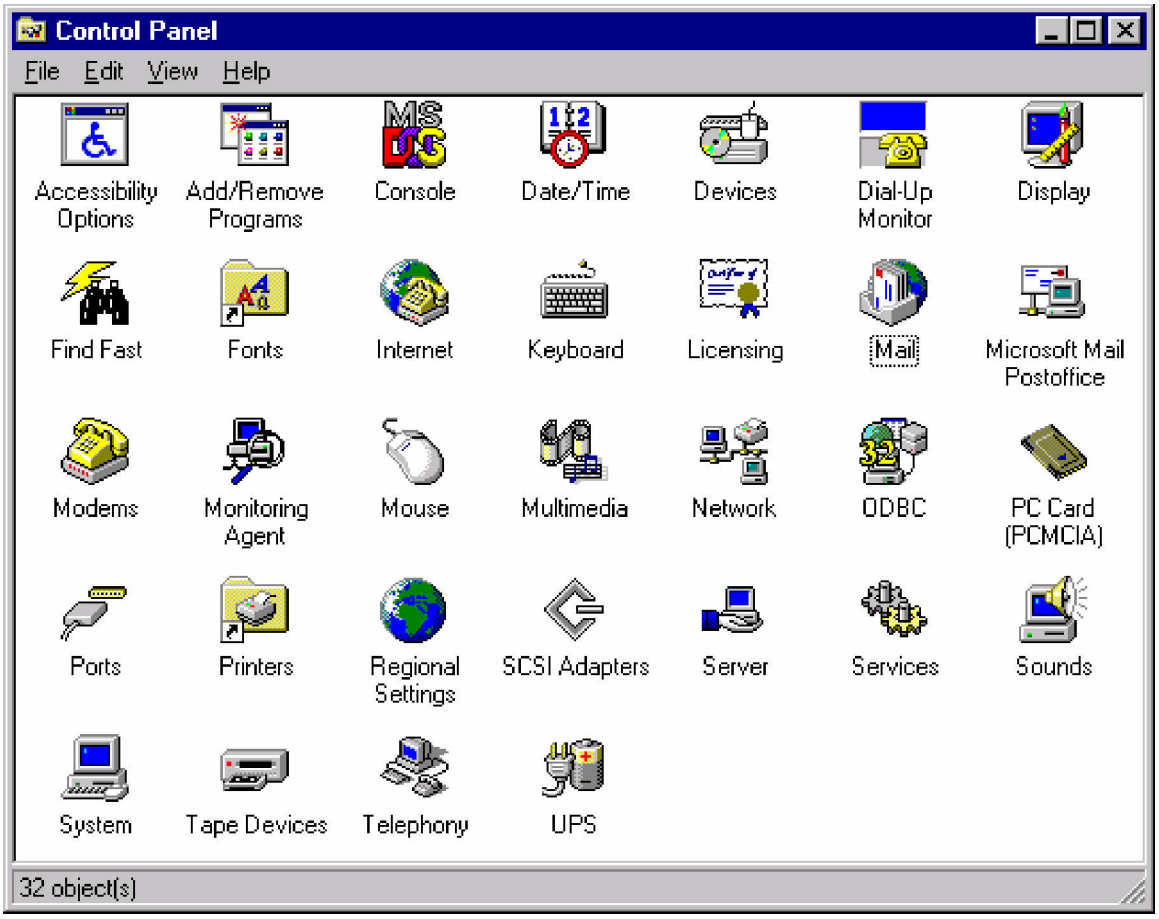
HotFixit

HotFixit ovat Service Packin jälkeen julkaistuja pikaisia korjauksia yhteen tiettyyn ongelmaan. Niitä ei *välttämättä* ole testattu oman ympäristösi kanssa samantyyppisessä ympäristössä, joten ota talteen päivitettävän tiedoston alkuperäinen versio ennen HotFixin asennusta!

HotFixit löytyvät tyypillisesti samasta jakelukanavasta kuin Service Packitkin.

3. OHJAUSPANEELI

Windows NT 4.0:n Ohjauspaneeli **Control Panel** on kokenut paljon muutoksia uudistuneen käyttöliittymän myötä. Tässä luvussa käydään läpi Ohjauspaneelin keskeisiä asetuksia palvelimen kannalta.



Windows NT 3.51:n **Windows NT Setup** on hajautettu seuraaviin Ohjauspaneelin asetuksiin:

- **Mouse** - hiiren asetukset
- **System**- käyttäjäprofiilien hallinta
- **Add/Remove Programs** - sovellusten asentaminen

- **Tape Devices** - nauhalaitteet
- **Keyboard** - näppäimistö

- **SCSI Adapters** - SCSI-sovittimet**.**

Ohjauspaneelin kuvakkeet ovat seuraavat (suluissa mainittu toimintaa mahdollisesti ohjaava Ohjauspaneelin laajennus (*Control Panel Extension*), joka löytyy **Winnt\System32**-hakemistosta):

- **Accessibility Options** - helppokäyttötoimintojen asetukset, liikuntarajoitteisille tarkoitetut käyttöä helpottavat asetukset (**access.cpl**)

- **Add/Remove Programs** - lisää/poista sovelluksia, uuden sovelluksen lisääminen (**appwiz.cpl**)

- **Console** - komentorivin ikkunan asetukset (**console.cpl**)

- **Date/Time** -päivämäärän ja ajan asetukset (**timedate.cpl**)

- **Devices** - käynnistää laiteohjaimet, lopettaa niiden käytön ja määrittää niiden käynnistystyypin

- **Dial-Up Monitor** - puhelinyhteyksien valvonta

- **Display** - näytön asetukset (**desk.cpl**)

- **Fonts** - kirjasinten käsittely

- **Internet** - Internet-yhteydet (**inetcpl.cpl**)

- **Keyboard** - näppäimistön asetukset

- **Licensing** - lisenssien asetukset (**liccpa.cpl**)

- **Mail** - sähköpostin asetukset (**mlcfg32.cpl**)

- **Microsoft Mail Postoffice** - työryhmätason postitoimiston asennus ja hallinta (**wppocpl.cpl**)

- **Modems** - modeemien asetukset (**modem.cpl**)

- **Monitoring Agent** - verkkomonitorin agentti (**bhctrl.cpl**)
- **Mouse** - hiiren asetukset (**main.cpl**)
- **Multimedia** - multimedian asetukset (**mmsys.cpl**)
- **Network** - lähiverkon työaseman asetukset (**ncpa.cpl**)
- **ODBC** - ODBC-ohjainten (*Open Database Connectivity*) käsittely (**odbccp32.cpl**)
- **PCMCIA** - PCMCIA-liitäntää käyttävän lisäkortin asentaminen ja hallinta (**devapps.cpl**)
- **Ports** - sarjaliitäntäportin valinta ja asetukset (**ports.cpl**)
- **Printers** - kirjoittimien asetukset
- **Regional Settings** - maa-asetukset (**intl.cpl**)
- **SCSI Adapters** - SCSI (Small Computer Systems Interface)-ohjainten määrittely
- **Server** - jaettujen resurssien seuranta (**srvmgr.cpl**)
- **Services** - palveluiden hallinta
- **Sounds** - äänten asetukset
- **System** - laitteiston ja käyttöjärjestelmän asetukset (**sysdm.cpl**)
- **Tape Devices** - nauhavarmistuslaitteiden laiteohjaimet ja asetukset
- **Telephony** - etäkäyttö- ja puhelinyhteyksien määrittely (**telephon.cpl**)
- **UPS** - keskeytymättömän virransyötön (UPS) asetukset (**ups.-cpl**).

Jokaisella Windows NT -käyttäjällä on oma käyttöympäristönsä, joka on tallennettu käyttäjän **profiiliin**. Kun käyttäjä kirjoittautuu järjestelmään, hän saa käyttöönsä omat asetuksensa, joita hän voi oikeuksistaan riippuen muuttaa. Listaan myös suomenkielisen Windows NT 4.0 -työaseman asetukset.

Eräitä **käyttäjäkohtaisia Ohjauspaneelin** (Control Panel) asetuksia ovat seuraavat:

- **Hiiri** (Mouse) - hiiren asetukset
- **Näyttö** (Display) - näytön taustakuviointi, kuvakkeiden väli
- **Näppäimistö** (Keyboard) - näppäimistön asetukset
- **Kirjoittimet** (Printers) - käyttäjäkohtaiset kirjoitinasetukset
- **Maakohtaiset asetukset** (Regional settings) - maa-asetukset
- **Järjestelmä** (System) - käyttäjän ympäristömuuttujat
- **Osoittimet** (Cursors) - osoittimen muoto
- **Ääni** (Sound) - äänet.

Eräitä **mikrokohtaisia** asetuksia ovat puolestaan seuraavat **Ohjauspaneelin** (Control Panel) asetukset: nämä vaikuttavat siis kaikkien kyseistä Windows NT -työasemaa / palvelinta käyttäviin käyttäjiin:

- **Fontit** (Fonts) - kirjasinlajin lisäys/poisto
- **Järjestelmä** (System) - laitteistokonfiguraatiot, käynnistysasetukset, järjestelmän ympäristömuuttujat
- **Portit** (Ports) - sarjaliitäntäportin valinta ja asetukset
- **Päivämäärä/Aika** (Date/Time) - muuttaa päivämäärän, ajan ja aikavyöhykkeen
- **Näyttö** (Display) - näytön asetukset ja tyyppi
- **Laitteet** (Devices) - oheislaitteiden ohjaimet

- **Palvelin** (Server) - palvelintoimintojen hallinta
- **Palvelut** (Services) - palvelut
- **UPS** - keskeytymättömän virransyötön (UPS) asetukset.

Voit käynnistää Ohjauspaneelin palvelimessa seuraavilla tavoilla:

- Valitsemalla **Start** | **Settings** | **Control Panel**
- Valitsemalla **My Computer**-ikkunassa **Control Panel**
- Valitsemalla **Control Panel** Explorer-näkymän resurssienhallinnassa.

Koska palvelimella ei tyypillisesti ole paikallisesti kirjautunutta käyttäjää (esimerkiksi käyttämässä Office-paketin sovelluksia), **palvelimen konfiguroinnin** kannalta erityistä merkitystä on seuraavilla asetuksilla:

- **Add/Remove Programs** - lisää/poista sovelluksia, uuden sovelluksen lisääminen - esimerkiksi virustorjunta- tai varmistusohjelmien asentaminen palvelimeen
- **Console** - komentorivin ikkunan asetukset
- **Devices** - käynnistää laiteohjaimet, lopettaa niiden käytön ja määrittää niiden käynnistystyypin
- **Dial-Up Monitor** - puhelinyhteyksien valvonta (jos **Remote Access Service** on asennettu), ks myös **Luku 7**
- **Licensing** - lisenssien asetukset
- **Microsoft Mail Postoffice** - työryhmätason postitoimiston asennus ja hallinta
- **Modems** - modeemien asetukset
- **Monitoring Agent** - verkkomonitorin agentti

- **Network** - lähiverkon työaseman asetukset
- **ODBC** - ODBC-ohjainten käsittely
- **Ports** - sarjaliitäntäportin valinta ja asetukset
- **Printers** - kirjoittimien asetukset
- **SCSI Adapters** - SCSI (Small Computer Systems Interface)-ohjainten määrittely
- **Server** - palvelintoimintojen hallinta; tietoja käyttäjien yhteyksistä ja resurssien käytöstä. Sen avulla voidaan muokata mikron kuvausta, saada luettelo mikroon kirjautuneista käyttäjistä sekä jaetuista ja avoimista resursseista. Tämän lisäksi hallitaan replikointia eli hakemistojen monistamista ja luetteloa järjestelmän hälytysten vastaanottajista. Tämä on etähallittavissa **Server Managerilla**
- **Services** - palveluiden hallinta. Lopettaa, aloittaa, keskeyttää tai jatkaa palvelimessa käytettävissä olevia palveluja, lähettää niille käynnistysparametreja ja määrittää palvelujen käynnistysasetukset. Tämä on etähallittavissa **Server Managerilla**
- **System** - laitteiston ja käyttöjärjestelmän asetukset, mm. sivutustiedoston ja käyttöjärjestelmän käynnistyksen asetukset
- **Tape Devices** - nauhavarmistuslaitteiden laiteohjaimet, niiden asentaminen ja asetukset
- **Telephony** - etäkäyttö- ja puhelinyhteyksien määrittely
- **UPS** - keskeytymättömän virransyötön (UPS) asetukset; se varmistaa järjestelmän sammuttamisen oikein virtakatkoksen aikana.

Nämä käsitellään seuraavaksi. Kaikki Windows NT 4.0:n Ohjauspaneelin asetukset on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä, joka keskittyy asetusten puolesta enemmän Windows NT 4.0:n työasemaversioon.

Add/Remove Programs

Add/Remove programs-kuvakkeen avulla Ohjauspaneeli mahdollistaa ohjelmien asentamisen ja niiden poistamisen.

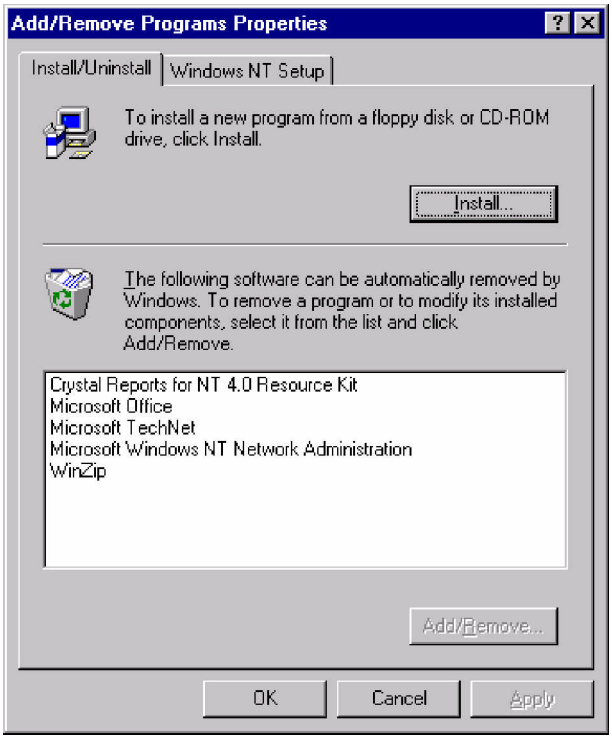
Välilehdet ovat seuraavat:

- **Install/Uninstall**-välilehden kautta lisätään uusi ohjelma kertomalla sen sijainti. Ikkunassa sen alapuolella näet ne asennetut Windows NT- tai Windows 95 -ohjelmat, jotka voidaan poistaa täysin niihin liittyvine tiedostoineen. Tämä vaatii sen, että ohjelma on Windows NT:lle tai Windows 95:lle sovitettu **32-bittinen versio**

- **Windows NT Setup**-välilehdessä voit Windows NT:n asennuksen jälkeen lisätä tai poistaa Windows NT:n osia.

Install/Uninstall

Install/Uninstall-välilehden kautta lisätään uusi ohjelma tai poistetaan asennettu ohjelma. **Install**-painikkeella käynnistetään uuden ohjelman asennusvelho (*Wizard*), joka kyselee asennusta varten tarvittavat tiedot. Jotta asennus tapahtuisi oikein, pitää sovelluksen olla rakennettu Windows NT:n käyttämälle asennustavalle. Muussa tapauksessa joudut asentamaan sovelluksen perinteisellä tavalla käynnistämällä sen asennusohjelma (tavallisesti **ASENNA.EXE** tai **SETUP.EXE**) joko komentoriviltä tai Explorer- resurssienhallinnalla.



Ikkunassa näet ne asennetut Windows NT- tai Windows 95 -ohjelmat, jotka voidaan poistaa täysin niihin liittyvine tiedostoineen tai joiden lisäosia voidaan asentaa.

Voit lisätä uuden ohjelman seuraavasti:

1) Valitse **Install**

2) Asenna levyke A:-asemaan tai CD-ROM asemaansa. Windows etsii asennusohjelmaa.

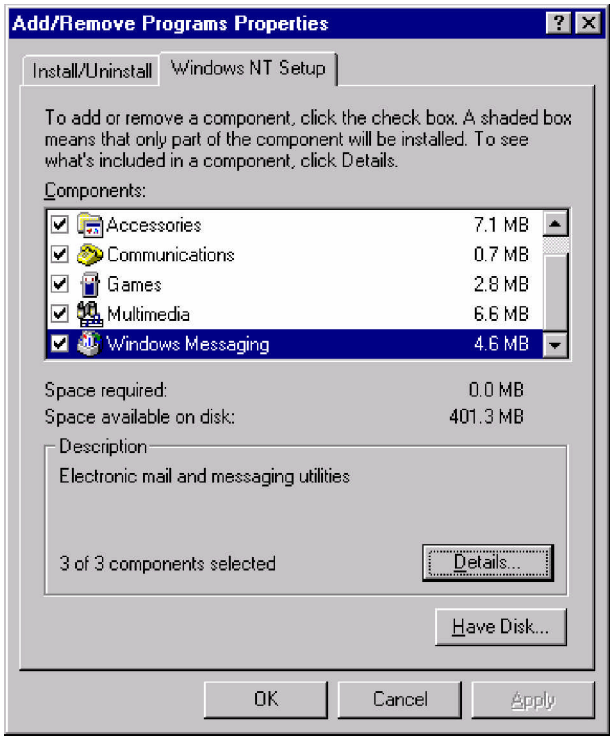
3) Kun asennusohjelma löytyi (**ASENNA.EXE** tai **SETUP.EXE**), voit painaa **Finish**. Tämän jälkeen sovelluksesta riippuva asennusohjelma käynnistyy. Seuraa sen ohjeita.

Ohjelman voit **poistaa** valitsemalla sen nimen listasta ja painamalla **Add/Remove**. Tämän jälkeen ohjelmasta riippuen se joko poistetaan samantien tai sinulta kysytään tarkemmin ohjelmaan liittyviä osia.

Voit myös tämän painikkeen kautta lisätä aiemman asennuksen jälkeen kyseiseen ohjelmaan liittyviä lisäosia.

Windows NT Setup

Windows NT Setup-välilehden avulla voit asentaa tai poistaa Windows NT -sovelluksia. Jos poistat sovelluksen, ota rasti pois sen kohdalta tai valitse poistettava ohjelma ja valitse **Details**.



Have Disk -painikkeella voit asentaa muita Windows NT:n komponetteja, jotka eivät tule Windows NT:n mukana. Se tehdään seuraavasti:

1) Valitse **Have Disk** ja selaa asennuslevyke tai -hakemisto

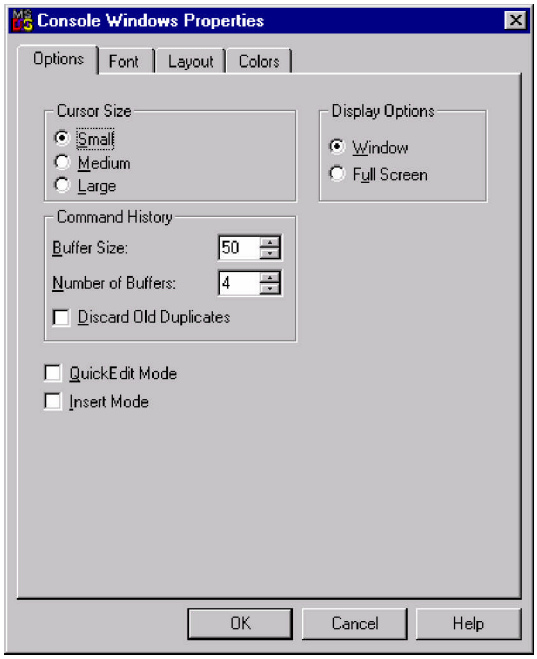
2) Paina **OK**. Tämän jälkeen näkyviin tulee ikkuna, jonka avulla voit sovelluksesta riippuen tarkentaa asennettavia osia. Paina **Install**

3) Asennuksen jälkeen sovellus tulee näkyviin **Windows NT Setup**-ikkunaan, josta voit sen myöhemmin poistaa.

Console

Consolen avulla voit määritellä komentorivi-ikkunan näytön asetukset.

Välilehdet ovat seuraavat:



- **Options** - voit asettaa kohdistimen koon **Cursor Size**, komentohistorian **Command History** puskurien koon ja lukumäärän, pikamuokkaustilan **QuickEdit Mode**, jolloin voit kopioida leikepöydälle tietoja helposti komentorivi-ikkunasta hiiren ja näppäimistön avulla sekä lisäystilan **Insert Mode**, jolloin komentoriville lisätään merkkejä. Lisäksi voit valita näytön asetukset **Display Options** ikkunassa **Window** tai koko näytössä **Full Screen**.

- **Font** - voit määritellä ikkunan fontin asetukset

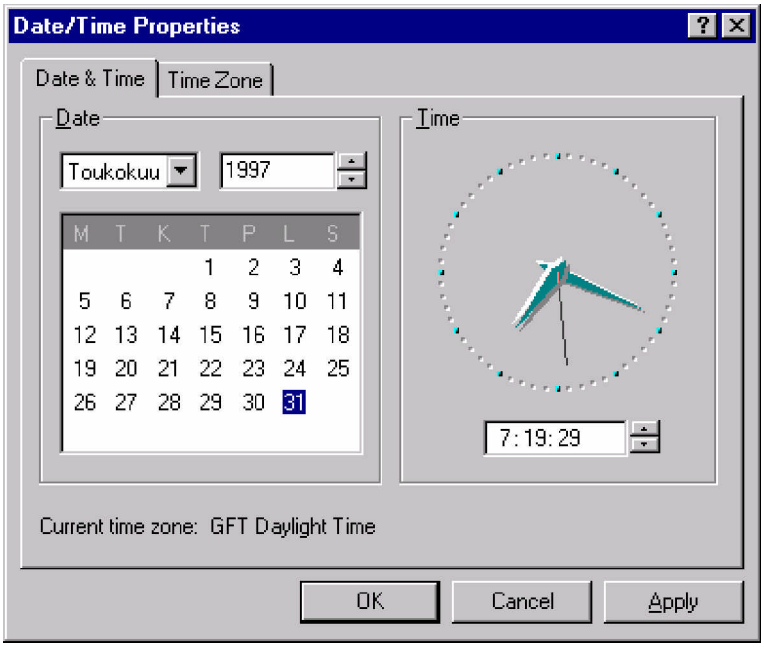
- **Layout** - ikkunan koon asetukset sekä sijainti

- **Colors** - tekstin ja taustan väriasetukset.

Date/Time

Päiväys asetetaan **Date/Time** -kuvakkeen avulla.

Voit myös kaksoisnapauttaa tehtäväpalkin päiväystä tai valita tehtäväpalkin pikavalikosta **Adjust Date/Time**.

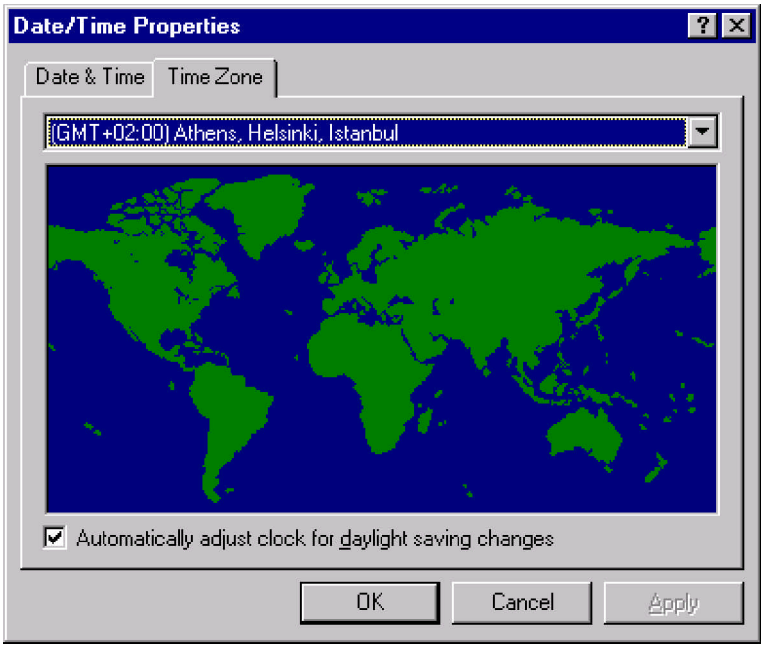


Välilehti **Date & Time** toimii myös yksinkertaisena kalenterina halutessasi katsoa tulevia päiviä ja niitä vastaavia viikonpäiviä. Kalenteri toimii vuosina 1980-2099.

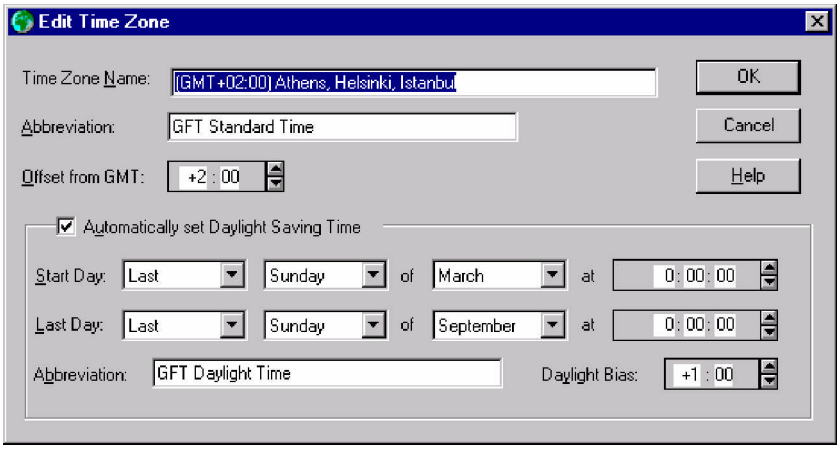
Voit muuttaa päiväystä valitsemalla hiirellä halutun vuoden, kuukauden tai päivän.

Jotta Windows osaisi vaihtaa kesä- ja talviajan oikein, pitää oikea aikavyöhyke olla valittuna. Se asetetaan välilehdessä **Time Zone**. Suomi kuuluu aikavyöhykkeeseen **GMT+2 tuntia** eli Suomi on edellä 2 tuntia Greenwichin keskiaikaa (*Greenwich Mean Time*).

Windows NT vaihtaa kesä/talviajan syyskuun ja maaliskuun viimeisenä sunnuntaina, mikä ei taas välttämättä ole EU-direktiivien mukaista.



Voit muuttaa aikavyöhykeasetuksia Resource Kitin **Windows NT Time Zone Editorin** avulla.



Devices

Devices-kuvakkeen avulla käynnistetään laiteohjaimet, lopetetaan niiden käyttö ja määritetään niiden käynnistystyyppi. Älä muuta näitä asetuksia vain kokeilumielessä!

Devices luettelee kaikki Windows NT:n tukemat laiteohjaimet sekä järjestelmään asennetut laiteohjaimet. Osa laiteohjainten nimistä on varsin kryptisiä, mutta joidenkin merkityksen voi päätellä suoraan nimestä. Pari esimerkkiä:

- **IDE CD-ROM** - jos poistat Windows NT:n asennuksen jälkeen IDE-väylään kytketyn CD-ROM:in, poista käytöstä myös IDE-CD-ROM:in **atapi** -laiteohjain

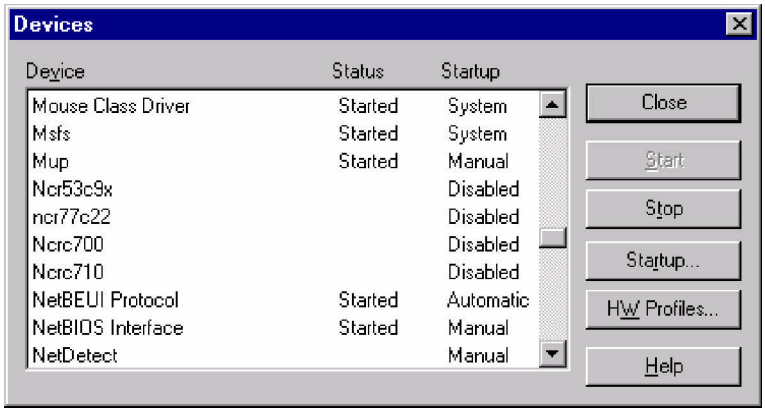
- **PCMCIA-korttien sovitin** (*PC-card Host Adapter*) - tarkista **pcmcia** -laiteohjaimen käynnistyminen sekä a.o. oheislaitteen laiteohjaimen asetukset

- **PCMCIA-korttikiintolevy** - tarkista **atdisk**-laiteohjaimen käynnistyminen.

Laitteiden käynnistäminen ja pysäyttäminen tehdään seuraavasti:

1) Valitse **Devices**-valintaikkunasta haluamasi laite. Jos laitteen **Status**-sarakkeessa on **Started** laitteen kohdalla, laiteohjain on ladattu muistiin ja käynnistetty - jos sarake on tyhjä, laiteohjainta ei ole ladattu

2) Valitse käynnistääksesi laiteohjaimen **Start**- tai pysäyttääksesi laiteohjaimen **Stop**-painike. Jotkin laitteet ovat välttämättömiä järjestelmän toiminnalle, eikä niitä voi siksi pysäyttää. Kun tällainen laite on valittuna, **Stop**-painike ei ole käytettävissä



3) Valitse **Sulje** (Close)-painike.

Laitteen käynnistystyypin määrittäminen edellyttää, että olet kirjautunut järjestelmään paikallisen **Administrators**-ryhmän jäsenenä.

Nyrkkisääntönä voidaan sanoa, että käynnistystyypit lähtevät kriittisimmästä tietokoneen käynnistyksestä **(Boot)** laitteen sulkemiseen käytöstä **(Disabled)**.

Laitteen käynnistystyypin määrittäminen tehdään seuraavasti:

1) Valitse **Devices**-valintaikkunasta haluamasi laite

2) Valitse **Startup...**-painike

3) Valitse **Startup Type**:

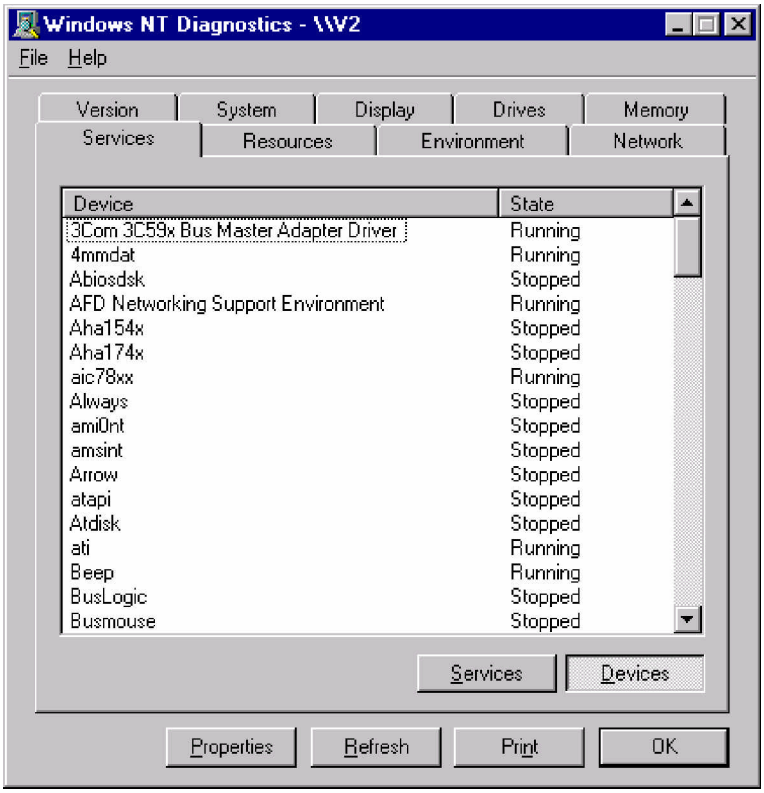
- **Boot** - tietokoneen käynnistys - tämän käynnistystyypin muuttaminen voi estää järjestelmän toiminnan!
- **System** - järjestelmä - tämän käynnistystyypin muuttaminen voi estää järjestelmän toiminnan!
- **Automatic** - automaattinen
- **Manual** - manuaalinen

- **Disabled** - ei käytössä

4) Valitse lopuksi **OK** ja valitse **Devices**-valintaikkunasta **Close**-painike.

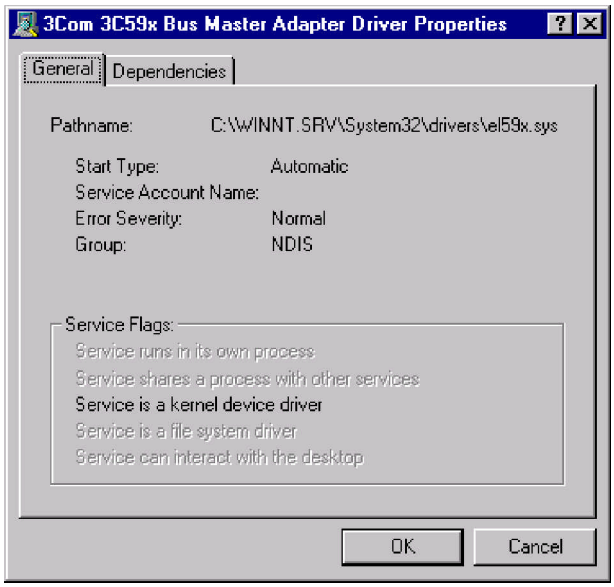
Hardware Profiles-painikkeen avulla voit valita missä laitteistoprofiileissa kyseinen oheislaite on käytössä. Palvelimet ovat yleensä kiinteästi asennettuja, joten tavallisesti niissä on määritelty vain yksi laiteprofiili.

Lisätietoja asennetuista oheislaitteista saat **Windows NT Diagnostics**-ohjelman avulla. Valitse **Services**-välilehti ja paina **Devices**. Näet myös oheislaiteohjainten tilan (**Running** / **Stopped**).



Tässä esimerkissä valitaan **3Com 3C59x Bus Master Adapter Driver**, mikä on verkkokortin laiteohjain.

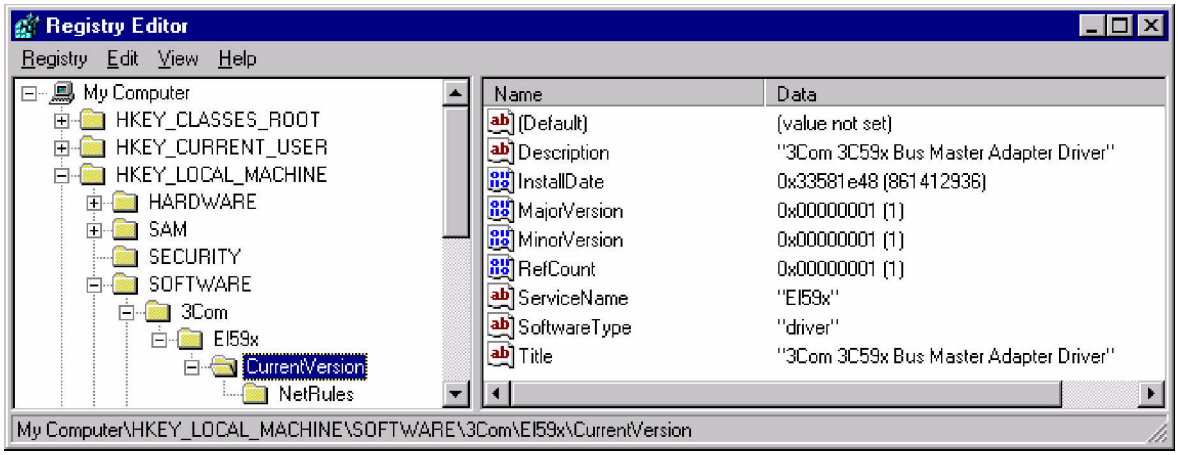
Valitsemalla **Properties** saadaan lisätietoja laiteohjaimesta.



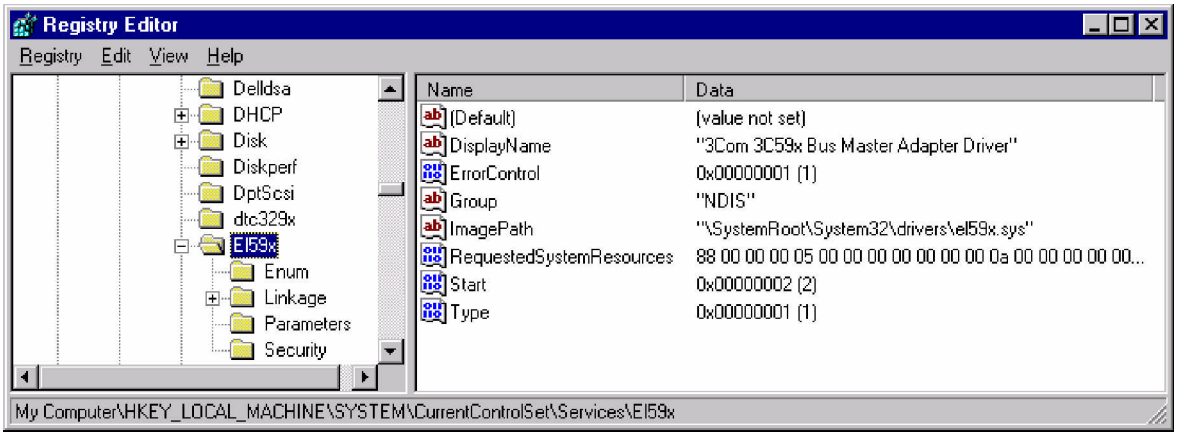
Nähdään itse laiteohjaimen fyysinen tiedostonimi (**el59x.sys**) sekä polku. Käynnistystyyppi on automaattinen.

Toki oheislaitteiden asetukset ovat rekisterissä.

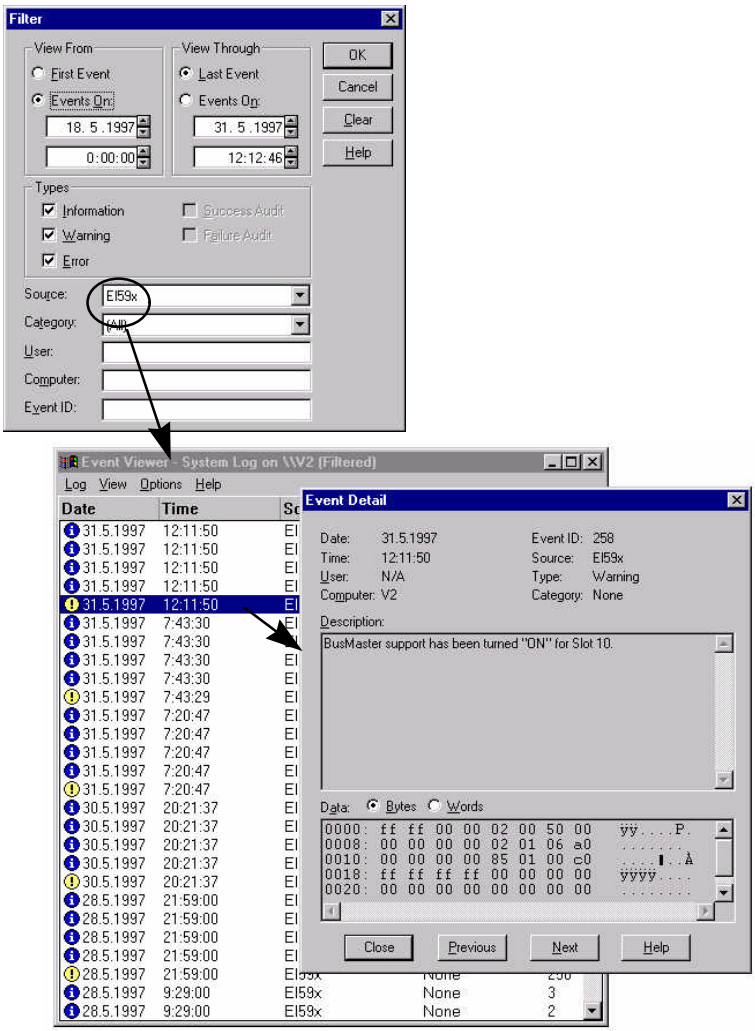
Polusta **HKEY_LOCAL_MACHINE\SOFTWARE\3Com\El59x \Current-Version** löytyy diagnostiikan näkemiä tietoja. Huomaa, että palvelun **ServiceName** nimi on **El59x**.



Laiteohjaimet löytyvät palveluina, polusta **HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet\Services löytyy** e.m. **El59x**.

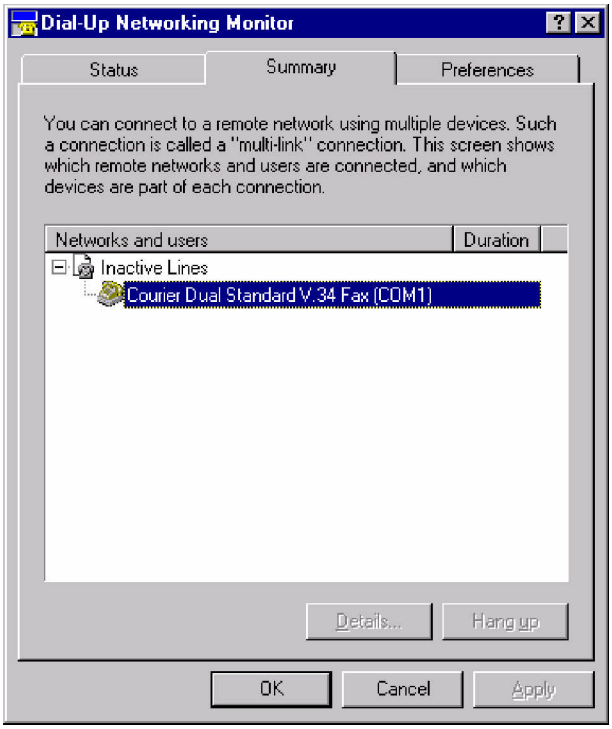


Vastaavasti **Event Viewer** -ohjelmalla voidaan tarkkailla **El59x**:n tuottamia tapahtumia (**Source**) järjestelmälokissa (**System**).



Dial-up Monitor

Ohjauspaneelin **Dial-up Monitorin** avulla valvotaan puhelinverkkoyhteyksien tilaa. Katso myös **Luku 7**.



Käytettävissä on kolme välilehteä:

- **Status** kertoo tämän hetkisen tilan lähetetyistä ja vastaanotetuista tavuista, virheiden määrän ja linjan tilan
- **Summary** on multilink-linjojen yhteenveto eli samanaikaisesti yhteen kohteeseen käytettyjen linjojen tila
- **Preferences** - äänimerkit virhetilanteissa ja Tehtäväpalkin indikaattorin asetukset.

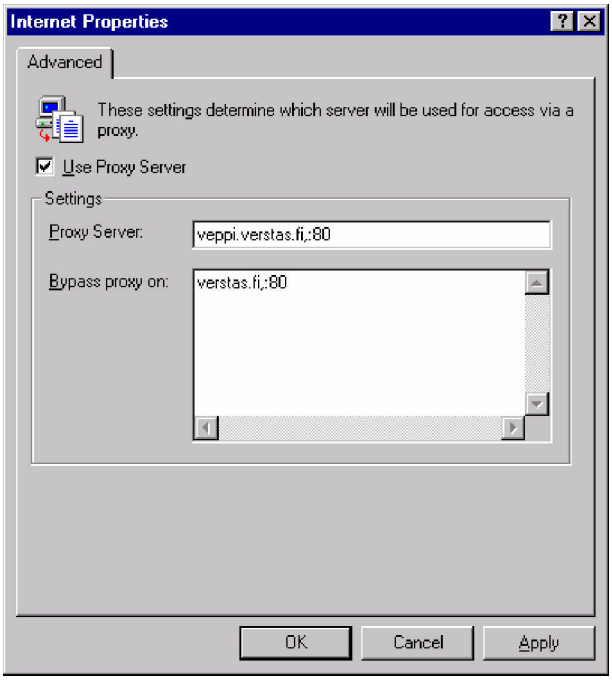
Internet

Internet-asetukset riippuvat asennetusta **Internet Information Server-palvelimen** ja **Internet Explorerin** versiosta. **Asetuksia on käsitelty myös luvussa 9.**

Internet-asetuksissa määritetään **välityspalvelimen** (*Proxy*) käyttö. Sen tarkoitus on ohjata Internet-liikenne yhden palvelimen kautta, jolloin liikenteen valvonta on mahdollista. Samalla voidaan suorittaa erilaisia tarkistuksia, pitää lokia jne. Asetus annetaan antamalla nimi ja **portti**.

Kyseessä on kyseisessä NT-koneessa annettava asetus! Tämä asetus on tehtävä kussakin NT-koneessa paikallisesti!

Vaikka olisitkin valinnut välityspalvelimen käyttöön, voit kuitenkin ohittaa välityspalvelimen **Bypass proxy on** antamalla halutun välityspalvelimen osoitteen ja portin pilkulla erotettuna, esimerkiksi **veppi.verstas.fi,:80**. Porttia **80** käyttää tavallisesti **http** ja porttia **443 https**.

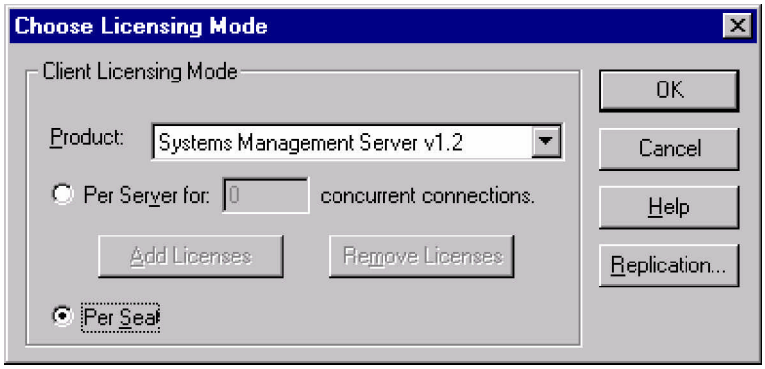


Licensing

Riippuen asennusvaiheen valinnasta, palvelin on asennettu joko **Per Server**- tai **Per Seat**-tyyppiseen lisenssimenettelyyn:

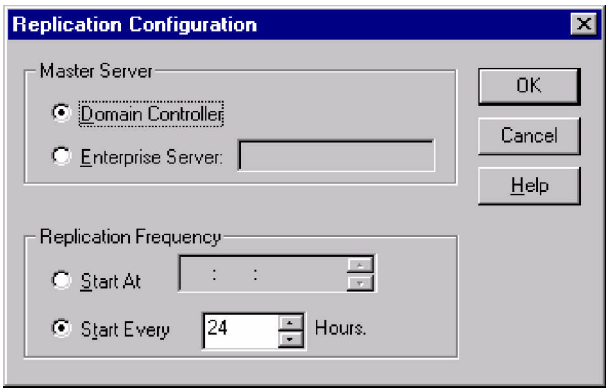
- **Per Server** - koskee tiettyä **samanaikaista käyttäjämäärää** BackOffice-ympäristöissä, mm. **Windows NT Server, Microsoft SQL Server**, **Microsoft SNA Server ja Systems Management Server**. Anna käyttäjämäärä ruutuun **Per Server for:**

- **Per Seat** - kyseessä on rajoittamaton käyttämäärä. Käytä **License Manager**-ohjelmaa asettaaksesi käyttäjät.



Asetuksia voit myöhemmin muuttaa **kerran** Control Panelin **Licensing**-kuvakkeella siten, että **Per Server** voidaan muuttaa **Per Seat** -tyyppiseksi.
Tällöin kyseessä on rajoittamaton käyttämäärä. Ennen muutosta kysytään vielä varmistus.

Painikkeella **Replication** voit määrittää monistuksen lisenssipalvelulle. Se voi olla PDC tai mikä tahansa palvelin, jolle kaikki verkon PDC:t rekisteröivät lisenssitietojaan.



Master Server on organisaation keskitetty päälisenssipalvelin . Se voi olla toimialueen **pääohjauskone** (*Primary Domain Controller*) tai mikä tahansa palvelin, jolle PDC:t ohjaavat lisenssitietojaan:

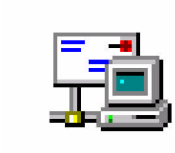
- **Domain Controller** - valitse tämä (se on oletus), jos palvelin on **Stand-alone Server** tai **varaohjauskone** (*Backup Domain Controller*), mutta ei ole **pääohjauskone**. Voit myös valita tämän **jos** palvelin on **pääohjauskone**, mutta **et** halua sen replikoivan lisenssitietojaan muualle

- Enterprise Server - palvelin on **Stand-alone Server** ja haluat sen replikoivan lisenssitietojaan lisenssitietojaan keskitettyyn lisenssipalvelimeen **tai** palvelin on **pääohjauskone**, ja **haluat** sen replikoivan lisenssitietojaan keskitettyyn lisenssipalvelimeen.

Replication Frequency määrittelee miten usein palvelimet antavat lisenssitietonsa. **Start every** -asetuksella haetaan aina uudelleen rekisteröintitiedot tietyn ajan välein. Minimi on kuuden tunnin välein.

Itse lisenssienhallinta tehdään **License Manager** -ohjelman avulla.

Microsoft Mail Postoffice



Postitoimisto voidaan luoda Windows NT -työasemaan, verkon palvelimeen tai toiseen työasemaan. Helpointa on kuitenkin luoda se käytössä olevaan palvelimeen; kannattaa lisäksi luoda vain yksi postitoimisto työryhmää kohti. Maksimimäärä on ehkä 50 - 100 käyttäjää postitoimistoa kohti - riippuen toki myös palvelimen laitteistosta ja käyttöjärjestelmästä.

Suuremmilla käyttäjämäärillä ja useiden postitoimistojen tullessa kysymykseen kannattaa harkita esimerkiksi MS Mail 3.5 -ohjelmistoa postitoimiston luomiseen ja hallintaan, tai sitten MS Exchange-palvelinta.

Postitoimiston luot seuraavasti:

1) Käynnistä ohjelma kaksoisnapauttamalla **Microsoft Mail Postoffice**-kuvaketta

2) Sinulta kysytään, haluatko luoda uuden vaiko kirjoittautua käyttäjäksi jo käytössä olevaan postitoimistoon. **Valitse Create a new Workgroup Postoffice**, niin luodaan uusi postitoimisto. Paina **Next**

3) Anna postitoimiston sijainti **\\palvelimennimi\jakonimi** tai jos olet ottanut yhteyden jaettuun hakemistoon, voit kirjoittaa esimerkiksi **M:**. Voit myös **Browsella** lähiverkkoa. Paina **Next**

4) Näet postitoimiston sijainnin. Paina **Next**

5) Määrittele seuraavaksi pakolliset valvojatilin tiedot:

- **Name** - koko nimi, maksimi pituus 30 merkkiä
- **Mailbox** - käyttäjän tunnus Mailissa, maksimi pituus 10 merkkiä
- **Password** - käyttäjän salasana Mailissa, maksimi pituus 8 merkkiä, oletuksena on **PASSWORD**

Voit halutessasi lisätä seuraavat tiedot:

- **Phone #1** - puh.nro, maksimi 32 merkkiä
- **Phone #2** - toinen puh.nro, maksimi 32 merkkiä, esim. fax, suora nro
- **Office** - toimisto, maksimi 32 merkkiä
- **Department** - osasto, maksimi 32 merkkiä
- **Notes** - mitä tahansa tekstiä, maksimipituus 128 merkkiä

6) Saat ilmoituksen postitoimiston luomisesta. Tämän jälkeen voit jakaa postitoimiston hakemiston käyttäjille

Valinnalla **Administer an existing Workgroup Postoffice** voit hallita luotua postitoimistoa. Toiminnot ovat samat kuin muissakin MS Mailin työryhmäversioissa. Käynnistettyäsi Mailin valvojatilin tunnuksella ja salasanalla voit siirtyä käyttäjien määrittelyyn:

- **Uuden käyttäjän lisääminen** onnistuu napauttamalla **Add user**
- Voit **muuttaa** aiemmin lisätyn käyttäjän määrityksiä valitsemalla käyttäjän nimen ja napauttamalla **Details**. Saat näyttöön käyttäjän nimen mukaisen syöttöikkunan. Tee tarvittavat muutokset ja napauta lopuksi **OK**
- Käyttäjän voit **poistaa** valitsemalla käyttäjän nimen ja napauttamalla **Remove User**. Sinulta pyydetään vielä kuittaus.

Modems

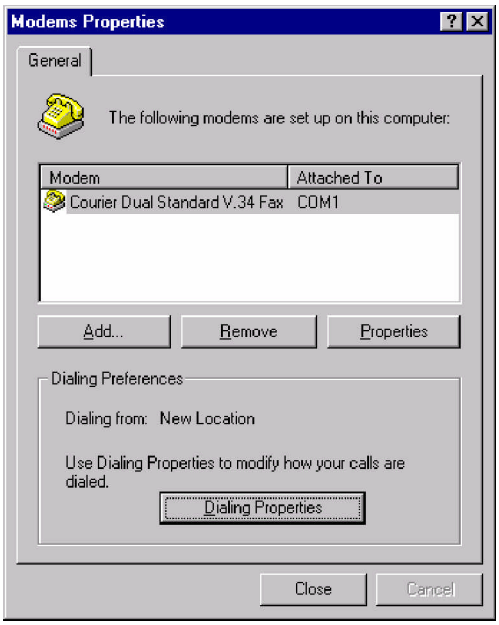
Modems-kuvakkeen avulla lisätään uusi modeemi, poistataan vanha tai muutetaan modeemin tai soittolinjan asetuksia.

Huomattavaa modeemien lisäämisestä:

- Windows NT-palvelimessa ei tulisi asentaa ja käyttää modeemeita ilman kunnollista suunnitelmaa siitä, miten puhelinverkkoyhteyksiä valvotaan ja kenelle ne sallitaan

- Sarjaportteihin kytketyt modeemit saattavat kuormittaa palvelinta huomattavasti. Jos haluat useita tukea useita modeemiyhteyksiä Windows NT:n **Remote Access Service**-palvelun avulla, hanki erillinen sarjaporttilaajennin (esim. **Digin EPC** tai **PC/x-kortti**). Nämä asennetaan Ohjauspaneelin **Network**-kuvakkeen avulla, samoin kuin ISDN-kortit

- Windows NT:n **unimodem**-tuki saattaa aiheuttaa ongelmia, jos modeemi ei tue Windows NT:n unimodem-standardia. Tällöin voit joutua poistamaan rekisteristä unimodem-tuen. Jos olet jo asentanut modeemit Windows NT 3.51:ssä ja päivität Windows NT 3.51:n 4.0:ään, tästä ei *pitäisi* tulla ongelmaa.



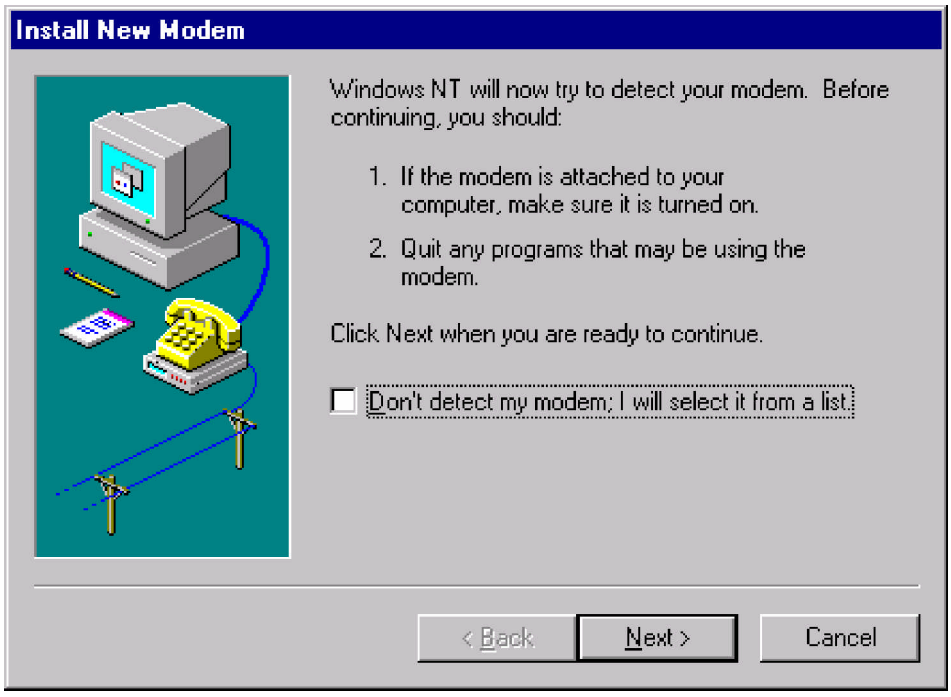
General-välilehti sisältää keskeiset modeemien asetukset. Painikkeet ovat:

- **Add** - modeemin lisääminen
- **Remove** - modeemin poistaminen
- **Properties** - modeemin asetukset
- **Dialing Properties** - yleiset soittoon liittyvät asetukset modeemin kautta soitettaessa.

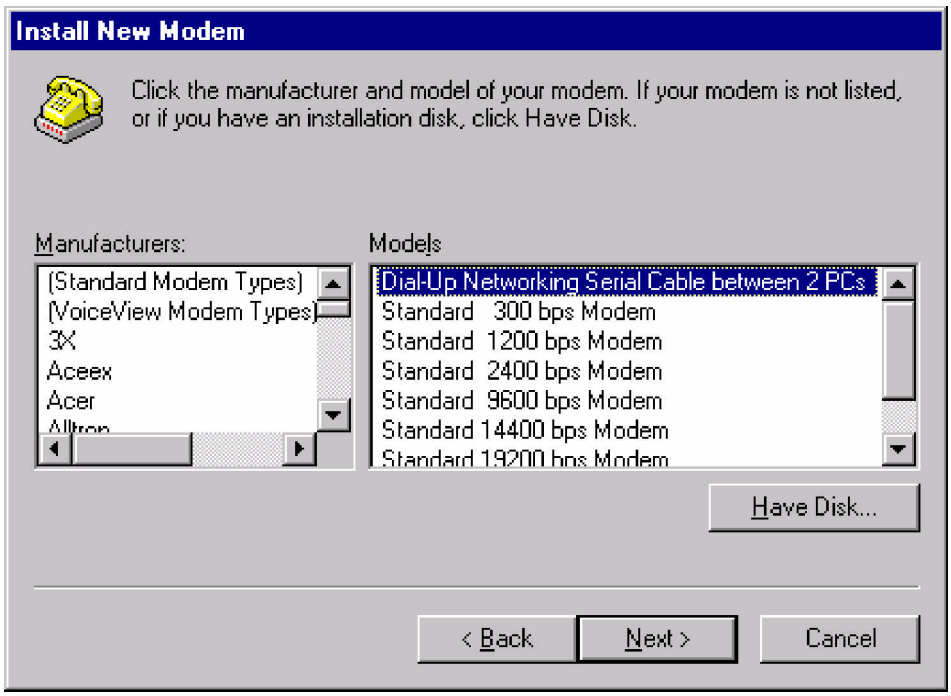
Uuden modeemin lisääminen tehdään seuraavasti:

1) Valitse **Add**-painike

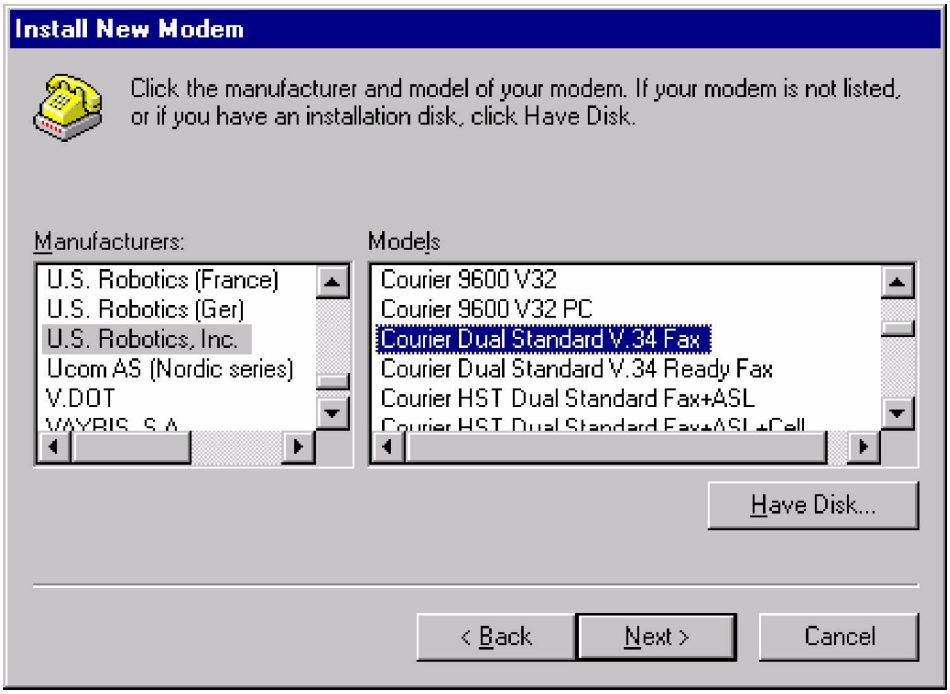
2) Windows tarjoaa mahdollisuutta automaattiseen asennukseen. Tavallisesti se kannattaakin valita; voit myös valita **Don t detect my modem**, jolloin valinnat on tehtävä itse



Tällöin voit muuten valita myös ns. **nollamodeemikaapelin** kahden mikron välille (**Dial-Up Networking Serial Cable between 2 PCs**).

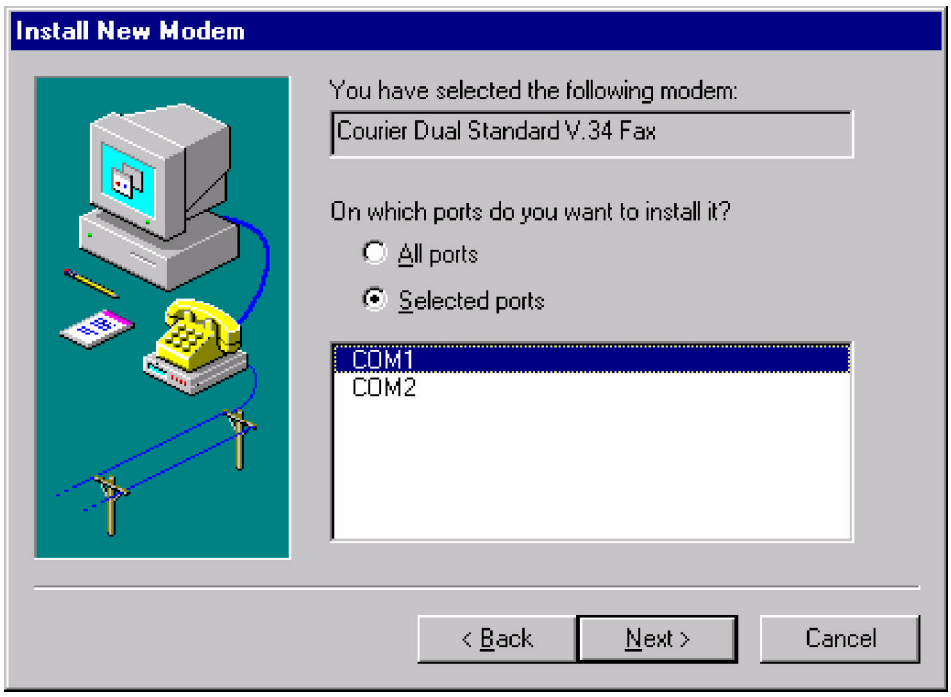


3) Jos valitsit automaattisen etsimisen, Windows NT etsii ja tunnistaa modeemin. Jos Windows ei tunnista modeemiasi, saat siitä ilmoituksen ja joudut itse asentamaan modeemin



Muussa tapauksessa Windows kertoo löytämänsä modeemin: jos tyyppi on oikea, paina siirtyäksesi eteenpäin **Next**: muuten voit muuttaa sen painamalla **Change**

4) Voit valita mihin sarjaportteihin haluat modeemin liittää.

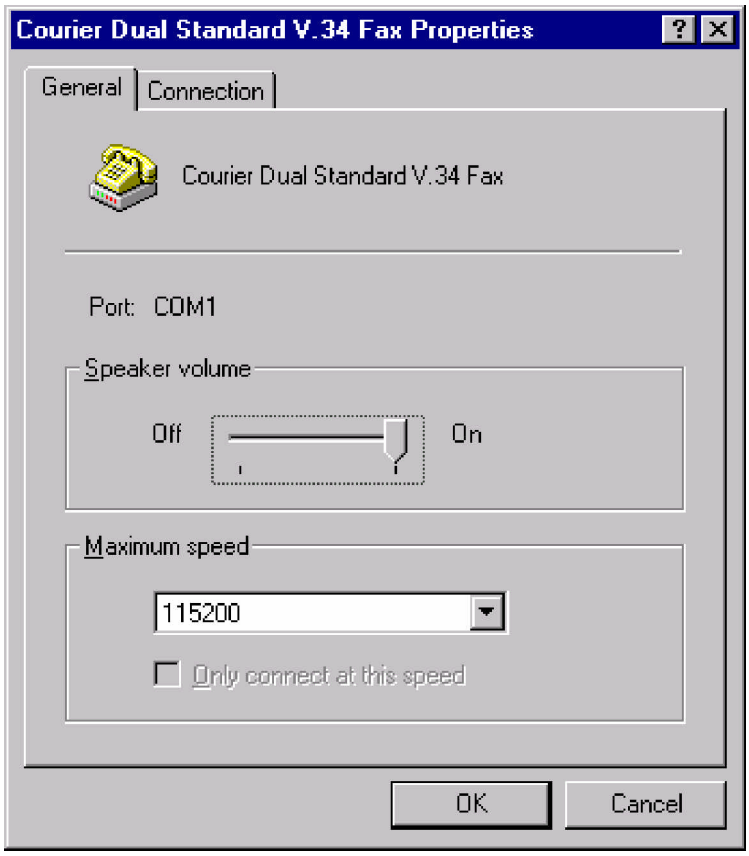


5) Valinnan jälkeen voit painaa **Next**. Tämän jälkeen voit lopuksi napauttaa **Finish**.

Modeemi poistetaan valitsemalla modeemi ja painamalla **Remove**.

Properties-painikkeella pääset käsittelemään modeemin asetuksia. **General**-välilehdessä nähdään modeemin käyttämä tietoliikenneportti eli sarjaliikenneportti (sarjaportti, *serial connection*) sekä päätelaitenopeus. Sarjaportit ovat tavallisesti **COM1**...**COM4**.

Voit myös asettaa kaiuttimen voimakkuuden.



Modeemiin liittyy oleellisesti sen siirtonopeus, joka ilmaistaan **bitteinä per sekunti** *(bps)*. Modeemien yhteydessä puhutaan usein myös **baudeista** *(baud)*, mikä toisinaan erheellisesti sekoitetaan tiedonsiirtonopeuteen jopa tietoliikenneohjelmissa. Baudi on modulointinopeuden yksikkö. Sekaannus johtuu pitkälti siitä, että vanhoissa 300 bps V21-modeemeissa modulointinopeus on 300 baudia. Vertailun vuoksi mainittakoon, että esimerkiksi 14 400 bps V32bis-modeemissa modulointinopeus on 2400 baudia.

Tärkeimmät siirtonopeudet ovat:

Siirtonopeus (bps)	Standardi
300	V.21
1200	V.22
2400	V.22bis
9600	V.32
14400	V.32bis
28800	V.34
65536	ISDN

Nykyaikaisilla nopeilla modeemeilla **päätelaitenopeus** voi olla moninkertainen linjanopeuteen verattuna. Päätelaitenopeus tarkoittaa **sarjaliitännän ja modeemin välistä nopeutta** eikä puhelinlinjalla käytettyä siirtonopeutta.

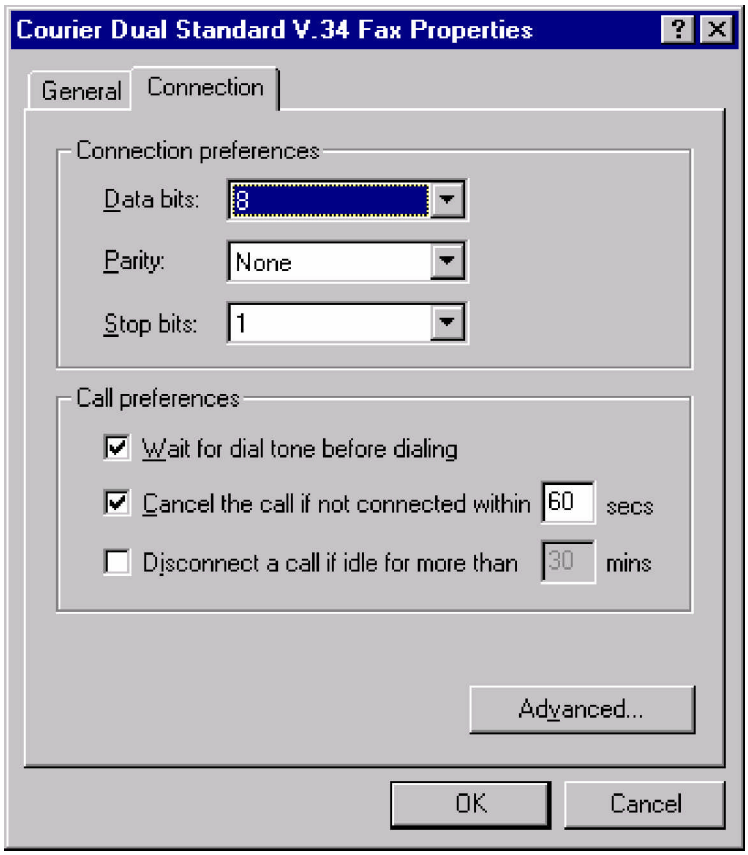
Päätelaitenopeus on normaalisti seuraavan taulukon mukainen:

Modeemin nopeus	Päätelaitenopeus
2400 bps	2400 bps
2400 (pakkauksella)	9600 bps
9600 bps	18200 / 38400 bps
14400 bps	19200 / 38400 / 57600 bps
28800 bps	19200 / 38400 / 57600 /115200 bps

Nopeuteen vaikuttaa **sarjaportissasi** käytössä oleva niin sanottu **UART-piiri**. Jos se on hidas **16540** tai **8250**, käytettävät nopeudet ovat korkeintaan **14 400 bps** luokkaa. Suurien päätelaitenopeuksien käyttäminen edellyttää, että sarjaliitännässä tai modeemissa on tehokas **puskurimuistilla varustettu UART-piiri**, esimerkiksi **16 bitin puskurilla varustettu 16550A** tai **32 bitin puskurilla varustettu 16650**. Vanhemmat/halvemmat UART-piirit **8250** ja **16450** eivät kunnolla sovellu V32bis- ja V34-modeemeille.

Voit tarkistaa asian käynnistämällä mikron DOS-käynnistyslevykkeellä ja **Microsoft Diagnostics** (MSD)-apuohjelmalla antamalla komentorivillä komento **MSD**. Ohjelman käynnistyttyä paina **C** (COM Ports), niin näet piirisarjojen tyypit.

Connection-välilehdessä määritetään, minkälaisia sarjaportin asetuksia käytetään. Yleisin on databittien asetus **Data bits** 8, pariteetti **Parity None** sekä stopbittejä **Stop bits** 1.



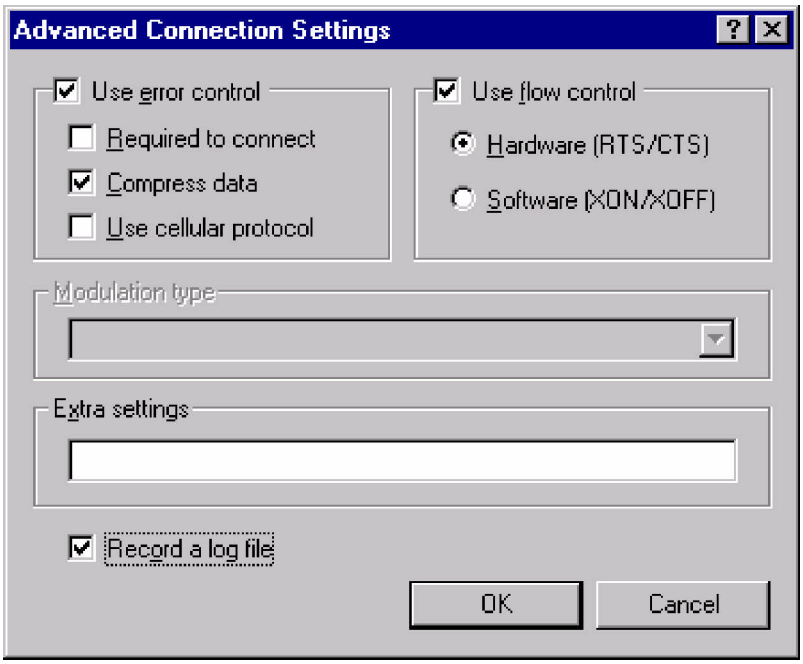
Soiton määritykset **Call preferences**-asetuksissa ovat seuraavat:

- **Wait for dial tone before dialing** odottaa valintaääntä ennen numeron valitsemista, mutta modeemin on tuettava tätä toimintoa

- **Cancel the call** peruuttaa soiton, jos yhteyttä ei saada annetun ajan kuluessa - modeemin on tuettava tätä toimintoa

- **Disconnect a call** katkaisee yhteyden annetun ajan kuluttua, jos linjalla ei siirretä dataa.

Advanced-painikkeella voidaan asetuksia muuttaa vieläkin syvemmällä tasolla.



Valinnat ovat:

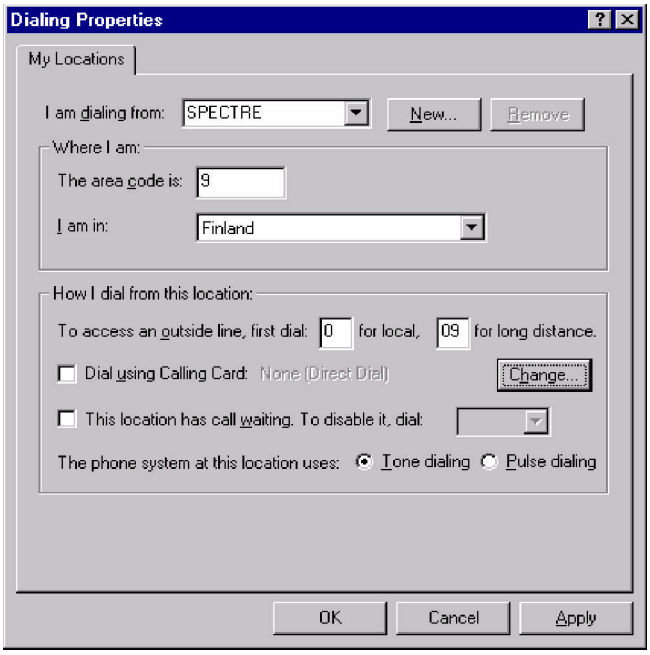
- **Use error control**-valintojen avulla virheenvalvonta otetaan käyttöön. Asetukset edellyttävät modeemin tukevan näitä toimintoja. Kyseessä on **V.42-standardi**, jota ei ole vanhemmissa modeemeissa. **Required to connect** pakottaa virheenvalvonnan käyttöön valitulla yhteydellä, mutta molempien modeemien on tuettava tällöin V.42-virheenvalvontaa. **Compress data** ottaa **V.42 bis**-pakkauksen käyttöön, jolloin **päätelaitenopeus voi mikron ja modeemin välillä olla modeemien välistä linjanopeutta** suurempi. Jos käytät matkapuhelimen datakorttia, voit **ehkä käyttää matkapuhelinprotokollaa** (Use cellular protocol)

- **Use flow control**-vuonhallinnalla määritellään modeemin ja mikron välinen tiedonsiirtomenetelmä. Valinnat ovat laitteistopohjainen **RTS/CTS** tai ohjelmistopohjainen **XON/XOFF**, mutta kaikki ohjelmat eivät välttämättä tue sitä. Laitteistopohjainen on suositeltavampi vaihtoehto, tavallisesti myös suorituskykynsä puolesta

- **Modulation type** on tavallisesti **Standard**, mutta USA:han soitettaessa voidaan valita käyttöön sikäläinen **Bellin standardi**

- **Extra settings**-riville voit kirjoittaa AT-komentokielen käskyjä, joita haluat modeemille välittää. Jos yhteys kulkee esimerkiksi puhelinkeskuksen kautta, pitää riville lisätä **x1**, jotta modeemi tunnistaa puhelinlinjan eri äänet oikein

- **Record a log file** tallentaa modeemiyhteyksien tiedot lokitiedostoon.



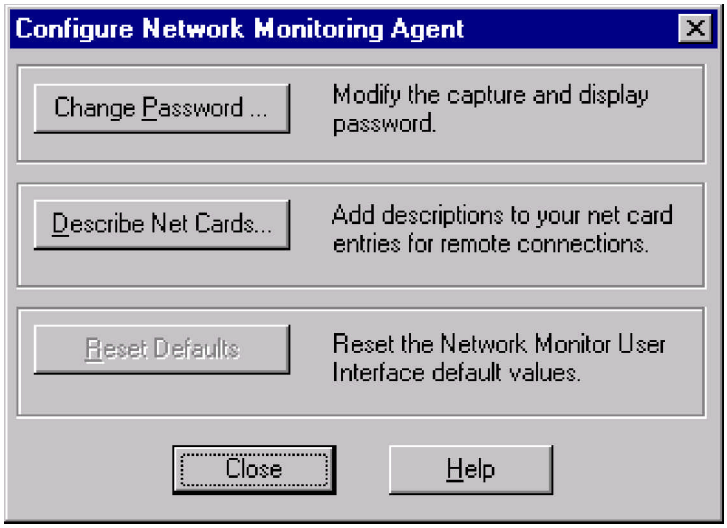
Dialing Properties määrittelevät modeeminkäyttöön liittyvät numeronvalintasetukset:

- **I am dialing from** - voit antaa sijainnin nimen tai luoda uuden painikkeella **New** tai poistaa asetukset painikkeella **Remove**

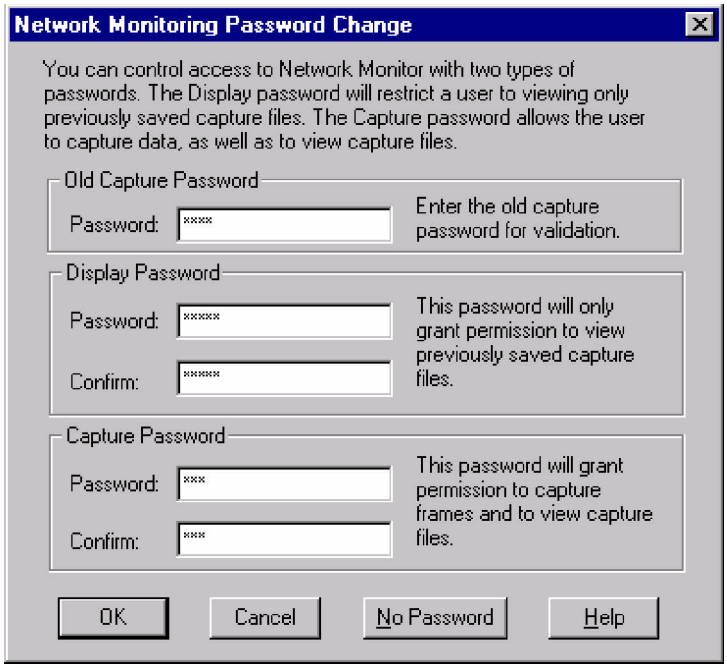
- Voit määritellä käyttöön puhelukortin **Calling Card** ja koputustoiminnon **call waiting**. Valitse tarvittaessa oikea valintamenetelmä: äänivalinta **Tone dialing** tai pulssivalinta **Pulse dialing**.

Monitoring Agent

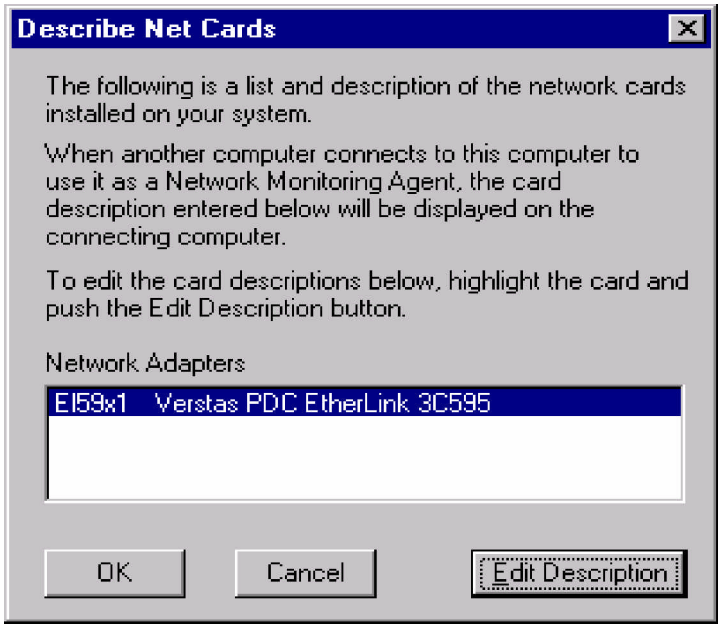
Tällä kuvakkeella voit asettaa palvelimen verkkomonitorille salasanat ja kuvauksen.



Valinnalla **Change password** voit muuttaa **Capture Passwordin**, jolla annetaan oikeus seurata kyseisen palvelimen verkkomonitoria. **Display Passwordin** avulla voidaan vain valvoa verkkomonitorilla tallennettuja lokeja ja **Capture Passwordin** avulla voidaan seurata verkkomonitoria.



Describe Net Cards-valinnalla voidaan antaa kuvaus verkkomonitorin verkkokortille.



Network

Verkkoasetukset määritellään **Network**-kuvakkeen avulla. Voit käyttää valintaa ja muuttaa asetuksia, jos olet **Administrators**-ryhmän jäsen.

Käytettävissä olevat välilehdet ovat:

- **Identification** tunnistetietojen asetukseen
- **Services** palveluiden määritykseen
- **Protocols** linjakurien (prokollien) asennukseen
- **Adapters** tietoliikenne- ja verkkokorttien asennukseen
- **Bindings** sidosten määritykseen edellisille.

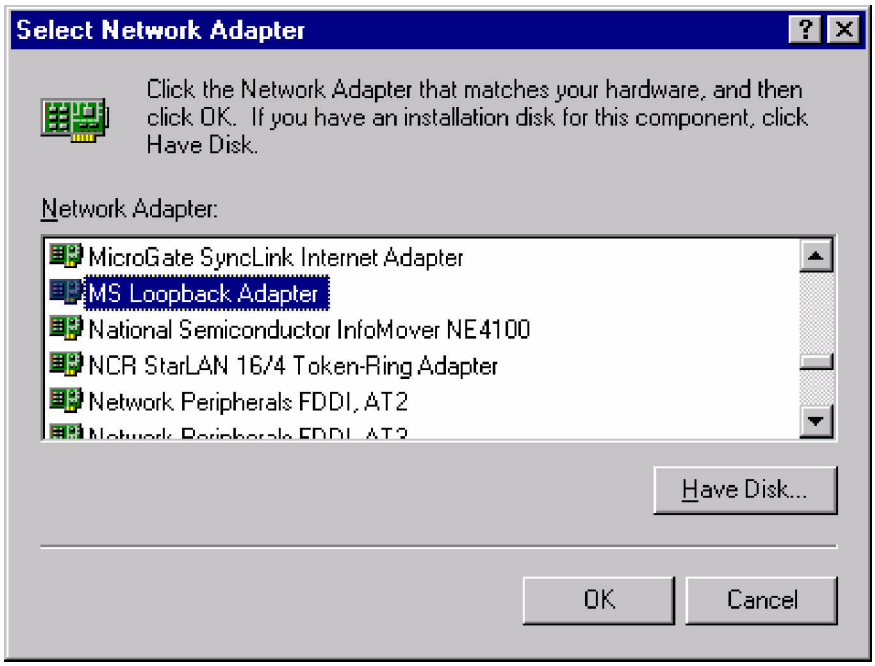
Huomattavaa:

- Verkkoasetusten määrittelyyn myös komentorivillä on käytettävissä **NET CONFIG WORKSTATION-** ja **NET CONFIG SERVER** -komennot, joista jälkimmäisellä voidaan piilottaa työasema/palvelin verkosta sekä ennen kaikkea määritellä **aikakatkaisu**

- Yhteenvedon asetuksista saat myös **Windows NT Diagnostics**-ohjelmalla

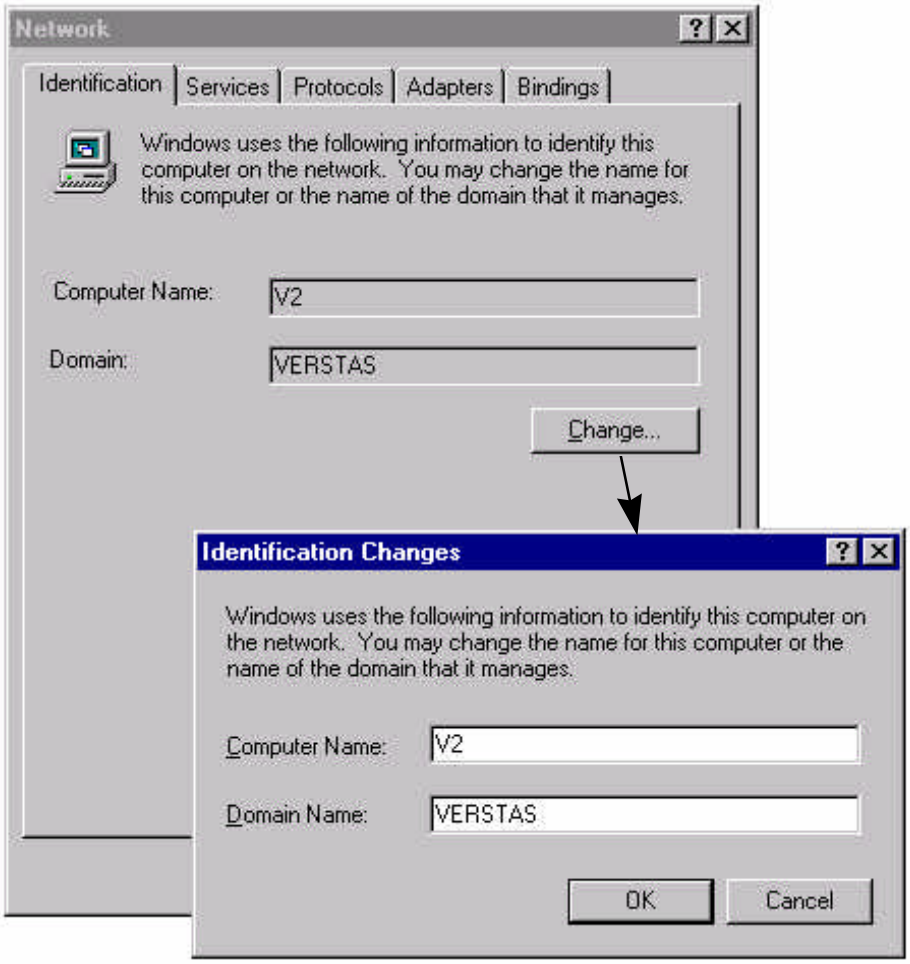
- Windows NT:n käyttäminen verkossa edellyttää, että määrität vähintään yhden verkkosovitinkortin ja verkko-ohjelmiston vähintään yhdelle verkkoprotokollaohjaimelle. Määritykset tehdään tyypillisesti asennusvaiheessa, mutta myöhemminkin voit muuttaa asetuksia seuraavassa esitellyllä tavalla, jos olet kirjautunut järjestelmään Administrators-ryhmän jäsenenä

- Et voi asentaa Windows NT-palvelinta ilman verkkotukea. Jos kuitenkin haluat asentaa palvelimen **ilman verkkokorttia**, asenna verkkokortiksi **MS Loopback Adapter** tai sopiva **Dial-Out Adapter**.



Identification

Identification-välilehdessä näet seuraavat tiedot:



- **Computer Name** - palvelimen nimi verkossa; nimen on oltava ainutkertainen

- Toimialue **Domain** tai työryhmä **Workgroup** - vain toinen näistä on näkyvissä; **ohjauskone** (*Domain Controller*)-tyyppinen palvelin voi olla liitettynä vain **toimialueeseen** (Domain), mutta **Stand-alone Server**-tyyppinen palvelin voi olla työryhmässä tai toimialueella.

Toimialueen muodostaminen edellyttää verkosta löytyvän kyseisen nimisestä toimialueesta **pääohjauskoneen** (*Primary Domain Controller*); työryhmän sen sijaan voi perustaa yksi tai useampi **Stand-alone Server**. Keskeisin ero on se, että työryhmässä ei ole keskitettyä käyttäjien hallin-

taa eli **jokaisessa** työryhmän **Stand-alone Serverissä** tai **NT-työasemassa** jokainen käyttäjä on määriteltävä erikseen; toimialueessa käyttäjien ja käyttäjätietojen hallinta on keskitetty palvelimelle.

Vaikka **Stand-alone Server** olisikin liitetty toimialueelle, siinä on silti hallittava käyttäjätunnukset erikseen **User Manager for Domains:lla**.

Change-painikkeella voit vaihtaa palvelimen nimeä tai Stand-alone Serverin liittymistä toimialueelle tai työryhmään.

Nimi muutetaan yksinkertaisesti antamalla uusi nimi **Computer Name**-kohtaan. Toimialueelle liittynyt **Stand-alone Server** tai NT-työasema pitää ottaa uudelleen toimialueelle palvelimen **Server Manager**-ohjelmalla valinnalla **Computer | Add to Domain**. Myös vanha **Stand-alone Server** tai NT-työasema pitää poistaa vanhasta toimialueesta valinnalla **Computer | Remove from Domain**.

Huomattavaa:

- Ohjauskoneen siirtäminen toiseen toimialueeseen saattaa olla mahdotonta! **Pääohjauskonetta** (*Primary Domain Controller*) ei voi siirtää toiseen toimialueeseen ilman uudelleenasennusta, ei tyypillisesti myöskään käyttäjien luomisen jälkeen muitakaan **ohjauskoneita** (*Backup Domain Controller*)

- **Ohjauskoneen** (*Domain Controller*) tapauksessa **Server Manager**-ohjelmalla valinnalla **Computer | Add to Domain** pitää ensin luoda uusi tili a.o. palvelimelle. Sen jälkeen vanha palvelin pitää poistaa valinnalla **Computer | Remove from Domain**

- Muutos ohjauskonepalvelimien siirtämiseen tulee vasta Windows NT 5.0:ssa

- **Stand-alone Serverissä** tai **NT-työasemassa** toimialueen vaihtaminen onnistuu.

Stand-alone Serverin tai NT-työaseman liittyminen työryhmään tehdään seuraavasti:

1) Valitse **Workgroup** ja kirjoita **Workgroup**-laatikkoon työryhmän nimi

2) Valitse **OK**.

Mitään muita erityistoimenpiteitä ei tarvita. Työryhmän nimen muuttaminen ei vaadi esimerkiksi NT:n uudelleenasentamista työasemassa.

Huomattavaa:

- Työryhmän nimi ei voi olla sama kuin tietokoneen nimi!
- Jos et ole varma toimialueen oikeasta nimestä tai muista valintaikkunan vaihtoehdoista, valitse aina **Workgroup** ja anna työryhmän nimeksi **Workgroup**, kunnes oikeat asetukset selviävät
- Jos työryhmään liittyneestä työasemasta halutaan käyttää toisen työaseman resursseja, on sama käyttäjätunnus määriteltävä toiseenkin työasemaan ja käyttäjätunnuksella on oltava oikeus käyttää kyseistä resurssia. Jos resurssi on jaettu ryhmälle **Everyone**, sitä pääsee käyttämään riippumatta käyttäjätunnuksesta
- Työryhmä-taso ei mahdollista keskitettyä käyttäjähallintaa
- On mahdollista ottaa käyttöön verkkoresurssi toisella käyttäjätunnuksella kuin sillä, jolla NT:hen on kirjauduttu, valinnalla **Yhdistä nimellä** (Connect as). Käyttäjätunnus annetaan muodossa **toimialue\käyttäjätunnus**.

Toimialueelle liittymisessä huomattavaa:

- Toimialueen muodostaminen edellyttää verkosta löytyvän **Windows NT Server**in, joka on liittynyt toimialueeseen. Ensimmäisen toimialueelle perustettavan palvelimen on aina oltava **toimialueen pääohjauskone** (*Primary Domain Controller*, PDC), joka muodostaa toimialueen keskitetyn käyttäjätietokannan ja muut palvelimet ovat **varaohjauskoneita**(*Backup Domain Controller*, BDC)-tyyppisiä palvelimia, jotka ylläpitävät kopiota käyttäjätietokannasta. Toimialueen muodostamiseen tarvitaan yksi PDC-palvelin. Toimialueessa on keskitetty käyttäjien hallinta ja käyttäjätietojen hallinta on keskitetty PDC-palvelimelle

- **Varaohjauskone** (*Backup Domain Controller*, BDC) on asennettava toimialueelle NT:n asennuksen yhteydessä

- NT-työaseman tai **Stand-alone Server**-palvelimen liittäminen toimialueelle tuo toimialueen jaetut resurssit a.o. NT-koneen käyttöön. Voit liittää NT-työaseman tai **Stand-alone Server**-palvelimen toimialueelle vain, jos olet kirjautunut sisään **Administrators**-ryhmän jäsenenä

- Lisäksi NT-työasemalla tai tai **Stand-alone Server**-palvelimella on oltava tili eli konetunnus (**Computer Account**) toimialueella. Jos tiedät **Administrators**-ryhmän jonkin käyttäjätunnuksen ja sen salasanan, voit lisätä toimialueelle NT-työaseman tai **Stand-alone Server**-palvelimen tilin samalla, kun liität a.o. NT-koneen toimialueelle. Muussa tapauksessa NT-kone pitää ottaa toimialueelle **Server Manager**-ohjelmalla. Tarvittaessa vanha konetunnus pitää poistaa samalla ohjelmalla!

Toimialueelle liittyminen NT-työasemassa tai **Stand-alone Server**-palvelimessa tehdään seuraavasti:

1) Valitse **Domain** ja kirjoita **Domain** -laatikkoon toimialueen nimi

Valitse **tarvittaessa** lisäksi **Create Computer Account in Domain** ja kirjoita **pääkäyttäjätason** (Administrator) käyttäjätunnus ja salasana sillä toimialueella johon liität työaseman. Tällöin järjestelmä lisää NT-koneen konetunnuksen automaattisesti toimialueelle, jos sillä ei ole vielä tiliä valmiina. Muussa tapauksessa NT-koneelle pitää luoda konetunnus **Server Manager**-ohjelmalla

2) Valitse **OK**. Kun toimialueelle liittyminen on onnistunut, näyttöön tulee siitä kertova viesti.

3) Et voi kuitenkaan kirjautua uudelle toimialueelle ennen kuin käynnistät NT:n uudelleen.

Huomattavaa:

- Kun olet liittänyt työaseman toimialueelle, kuka tahansa tarvittavat käyttöoikeudet omistava käyttäjä voi käyttää sitä mistä tahansa toimialueelle määritellystä työasemasta.

- NT-työaseman **Käyttäjien hallinnalla** (User Manager) tai **Stand -alone Server**-palvelimen **User Manager for Domainsilla** kannattaa heti toimialueelle liittämisen jälkeen tehdä seuraavat tarkistukset:

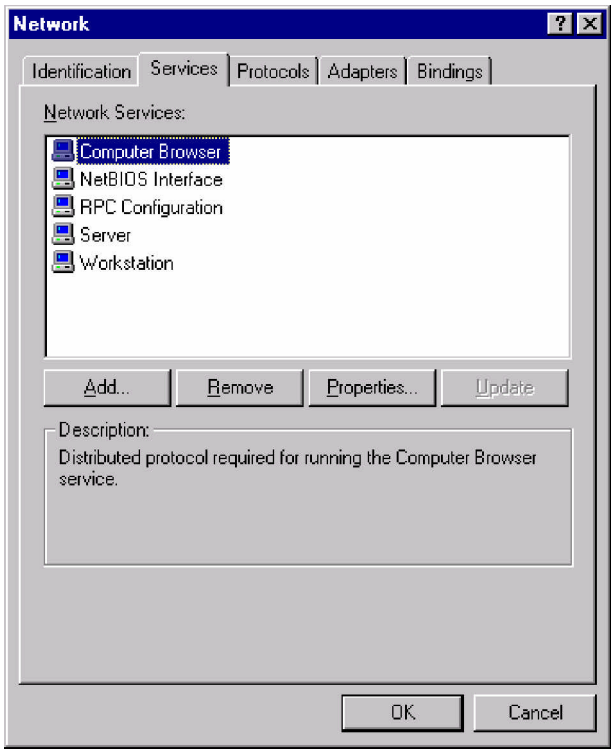
- Kun NT-kone on liitetty toimialueelle, kannattaa yleensä paikallisessa käyttäjäryhmässä **Käyttäjät** (Users) olla mukana kyseisen toimialueen yleinen käyttäjäryhmä **Domain Users**. Tällä varmistetaan paikallisten resurssien käyttöoikeus riippumatta siitä, kuka toimialueen käyttäjä on kirjautunut a.o. NT-koneeseen

- Edelleen paikallisessa **Järjestelmänvalvojat** (Administrators)-ryhmässä kannattaa olla mukana toimialueen **Domain Admins**-ryhmä. Tällä varmistetaan se, että toimialueen pääkäyttäjien tunnuksilla voi hallita a.o. NT-konetta.

Services

Services-välilehdessä määritellään verkkopalvelut.

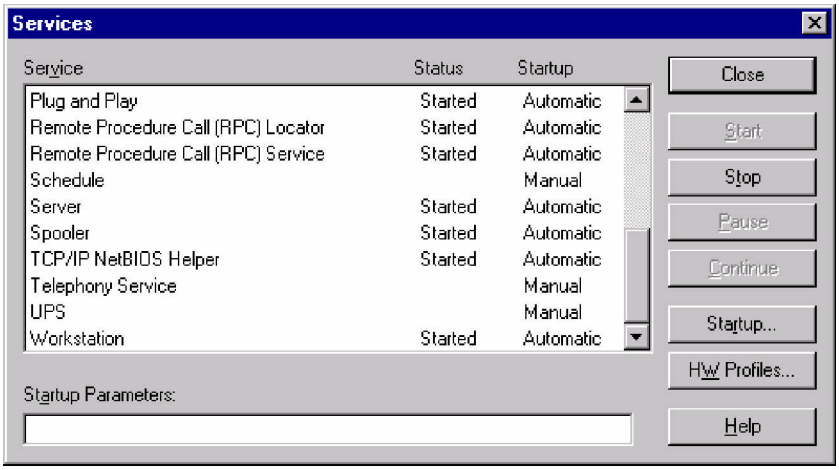
Network Services -lista näyttää asennusvaiheessa tai myöhemmin lisätyt verkkopalvelut.



Tyypilliset ja tarpeelliset **peruspalvelut** palvelimessa ovat:

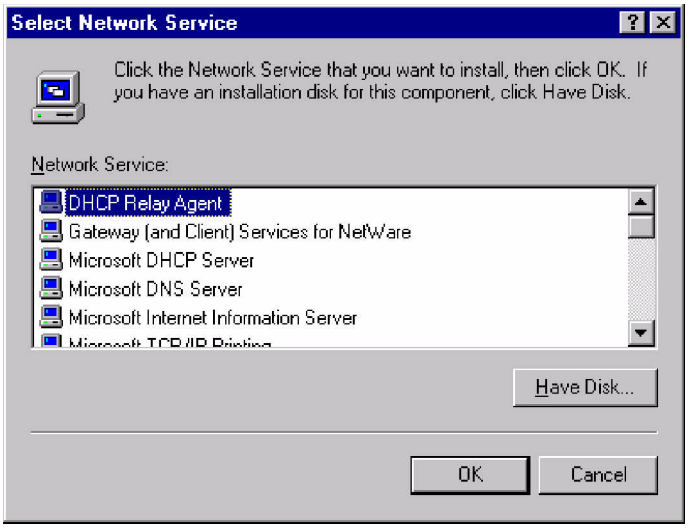
- **Computer Browser** - selauspalvelu
- **NetBIOS Interface** - tämän avulla työasemaa voidaan mm. etähallita ja suorittaa NetBIOS-sovelluksia (esimerkiksi NET-komennot)
- **RPC Configuration** - etäproseduurikutsupalvelun (RPC) -asetukset, RPC mm. mahdollistaa prosessien suorittamisen etäkoneessa
- **Server** - palvelimen resurssien jakamisen mahdollistava komponentti
- **Workstation** - työaseman verkkokäytön mahdollistava komponentti ja perusta muille palveluille.

Näet osan näistä palveluista myös Ohjauspaneelin **Services**-kuvakkeen avulla:



Palveluiden hallinta on mahdollista myös komentorivin **NET START-** ja **NET STOP** -komennoilla.

Painikkeella **Add** voit lisätä verkkopalveluita:



Lisättäviä palveluita ovat mm. seuraavat:

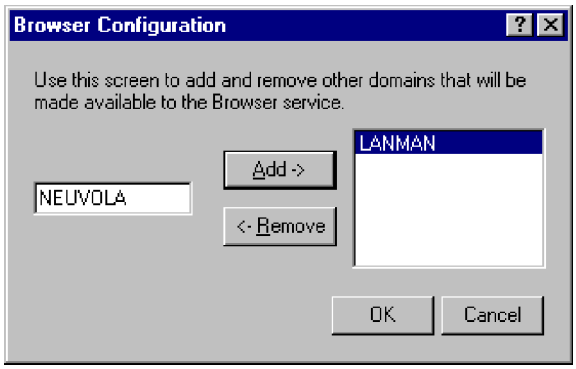
- **DHCP Relay Agent** - DHCP-palvelimen *(Dynamic Host Control Protocol)* jakamien IP-osoitteiden välityspalvelu
- **Gateway (and Client) Services for NetWare** - yhdyskäytävä- ja työasematuki NetWare-verkolle

- **Microsoft DHCP Server** - IP-osoitteita jakava DHCP-palvelin
- **Microsoft DNS Server** - DNS-nimipalvelu (*Domain Name Service)*
- **Microsoft Internet Information Server** - WWW-, Gopher- ja FTP-palvelin
- **Microsoft TCP/IP Printing** - tulostuspalvelu mm. Unix-palvelimiin ja -työasemiin
- **NetBIOS Interface** - tämän avulla työasemaa voidaan mm. etähallita ja suorittaa NetBIOS-sovelluksia (esimerkiksi NET-komennot)
- **Network Monitor Agent** - verkkomonitorin agentti
- **Network Monitor Tools and Agent** - verkkomonitorin työkalu ja agentti
- **Remote Access Service** - tuki etäkäytölle, sekä asiakas että palvelin
- **Remoteboot Service** - tuki levyttömille työasemille
- **RIP for Internet Protocol** - reitittimien käyttämän RIP (*Routing Information Protocol*)-protokollan tuki IP-protokollalle
- **RIP for NWLink IPX/SPX compatible transport** - reitittimien käyttämän RIP-protokollan tuki IPX/SPX-protokollalle (*Internet Protocol eXtended/Service Protocol eXtended*)
- **RPC Configuration** - RPC (*Remote Procedure Call*) mahdollistaa prosessien suorittamisen etäkoneessa
- **RPC Support for Banyan** - RPC-tuki Banyan Vines -verkolle
- **SAP Agent** - SAP (*Service Advertising Protocol*) on Novellin protokolla, jolla mainostetaan Novell-palvelimen tarjoamia palveluita yleissanomien (*broadcast*) avulla. SAP-agentti osaa välittää näitä yleissanomia

- **Server** - resurssien jakamisen mahdollistava komponentti
- **Services for Macintosh** - palvelimen Macintosh-tuki
- **Simple TCP/IP Services** - TCP/IP-apuohjelmat
- **SNMP Service** - SNMP (*Simple Network Management Protocol*) tarjoaa SNMP-hallintatuen
- **Windows Internet Name Service** - NetBIOS-nimipalvelu
- **Workstation** - työaseman verkkokäytön mahdollistava komponentti ja perusta muille palveluille.

Lisättyäsi palvelun palvelin pitää käynnistää uudelleen. Joitakin palveluita voit konfiguroida valitsemalla palvelun ja painamalla **Properties**.

Computer Browser



Computer Browser -selauspalvelu pitää luetteloa toimialueista/työryhmistä sekä toimialueen/työryhmän työasemista/palvelimista ja se voidaan asettaa pitämään listaa myös LAN Manager-toimialueista. Kirjoita toimialueen nimi ja paina **Add**. Tarvittaessa voit poistaa toimialueen selailun valitsemalla sen nimen listasta ja painamalla **Remove**.

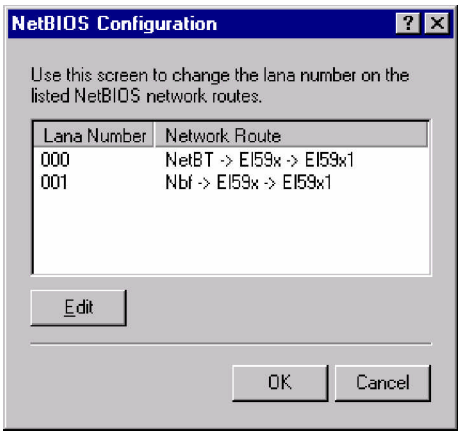
Voit lisätä reitinverkoissa myös toisten toimialueiden nimiä, joiden työasemia tai palvelimia **ei** ole palvelimen kanssa samassa aliverkossa.

NetBIOS Interface

NetBIOS Interface -liittymän **LANA** (*LAN Adapter*) -asetuksia voit muuttaa tarvittaessa, esimerkiksi *jos* jokin sovellus *nimenomaan* vaatii jonkin tietyn LANA-numeron.

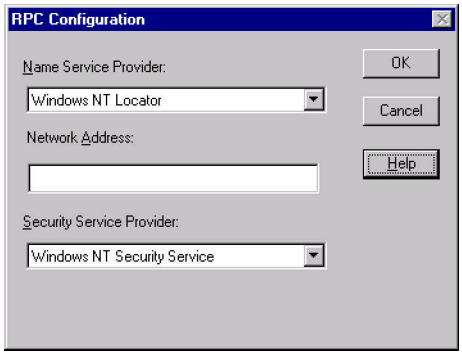
Alunperin LANA tarkoitti fyysistä verkkokorttia, joita saattoi olla mikrossa kaksi kappaletta. Ensimmäinen verkkokortti oli LANA, jota sovellukset käyttivät oletuksena. Jos mikroon lisättiin toinen verkkokortti, sovelluksia voitiin määrittää käyttämään tätä nimenomaista verkkokorttia.

Microsoft on laajentanut alkuperäisen NetBIOS:in käyttämään myös muita kuin NETBEUI-protokollaa, itse asiassa LANA tarkoittaa tiettyä protokollaa tietyssä verkkokortissa. Esimerkiksi kahden verkkokortin ja kahden protokollan tapauksessa on käytettävissä neljä LANA:a.



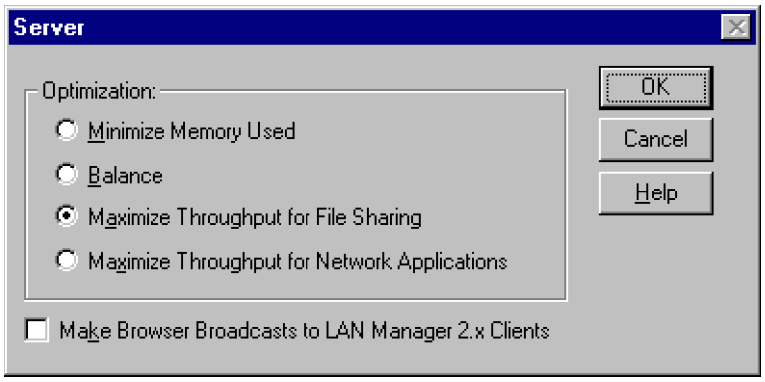
RPC Configuration

RPC:n nimipalvelutoimittajana **Name Service Provider** on oletuksena **Windows NT Locator**. Jos valitset **DCE Cell Directory -palvelun** voit asettaa myös verkko-osoitteen. Lisäksi voit asettaa suojauspalvelutoimittajan **Security Service Provider**.



Server

Palvelinpalvelun asetuksissa voit muuttaa verkkoyhteyksille ja käynnistetyille sovelluksille varattavan muistin määrää sekä lisäksi hallita yhteyksiä verkon LAN Manager-version 2.x -palvelimille. Voit asettaa jonkin seuraavista asetuksista:

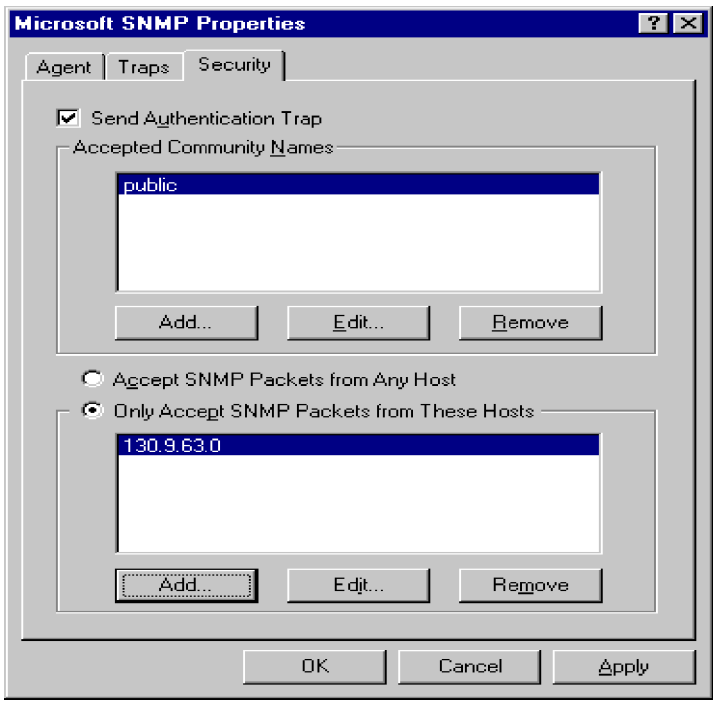


- **Minimize Memory Used** - yhteyksiä on enintään 10 kpl
- **Balance** - yhteyksiä on enintään 64 kpl (myös NetBEUI:n oletusasetus)
- **Maximize Throughput for File Sharing** - tiedostojen jakotoiminnot saavat enemmän aikaa
- **Maximize Throughput for Network Applications** - jos mikrossa on esimerkiksi tietokantapalvelin, kuten **SQL Server**
- **Make Browser Broadcasts to LAN Manager 2.x Clients** - yleissanomien lähetys LM-tyyppisesti - valitse, jos haluat, että LM-palvelimet ja työasemat voivat selata NT-mikroja.

SNMP

Jos asensit **SNMP**:n, voit **Agent**-, **Traps**- ja **Security**-välilehdillä määritellä SNMP:n asetukset. Nämä riippuvat omasta verkkoympäristöstäsi.

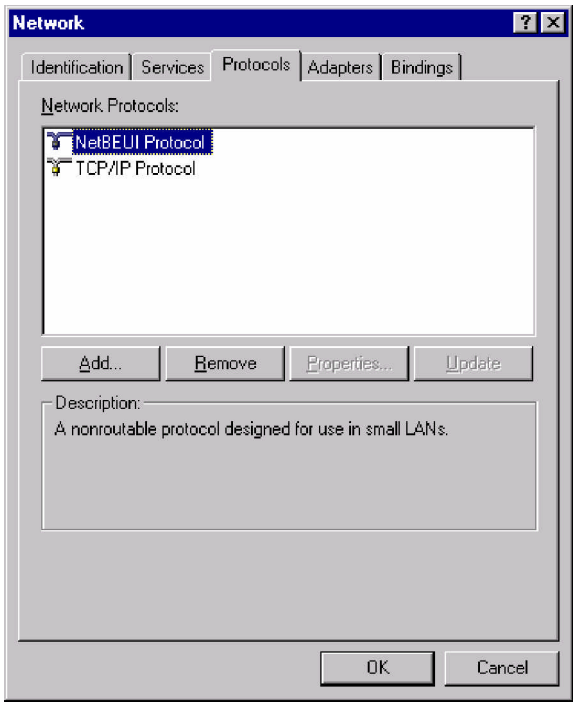
Security-välilehdellä voit antaa nimen, jolle valvontailmoitukset **Traps** lähetetään: anna **hyväksytyt yhteisönimet** kohdassa **Accepted Community Names**. Tavallinen tällainen on **public**. Voit myös määritellä SNMP-valvontatyöasemien IP-osoitteet.



Protocols

Protokollan eli linjakurin avulla eri laitteet kommunikoivat keskenään. Asennetut protokollat näet **Network Protocols**-listassa.

Painikkeella **Add** voit lisätä protokollan, **Remove** poistaa, **Properties** antaa mahdollisuuden määritellä protokollan asetuksia ja **Update** tarjoaa mahdollisuuden päivittää protokolla.



Käytettävissä olevat protokollat ovat seuraavat:

- **Apple Talk Protocol** tarvitaan **Apple MacIntosh** -yhteyksiin
- **DLC Protocol** - DLC (*Data Link Control*) - tarvitaan IBM-keskuskoneyhteyksiin. Myös eräät verkkokirjoittimet tukevat tätä protokollaa
- **NetBEUI Protocol** on varsin yleinen, mutta se ei toimi reitittimerkoissa. Tämä rajoittaa sen tehokkaan käytön vain suhteellisen pieniin verkkoihin
- **NWLink IPX/SPX Compatible Transport** - Novell NetWare-verkoissa käytetty protokolla
- **Point to Point Tunneling Protocol** - päästä-päähän käytäntö, protokolla, jota käytetään esimerkiksi lähiverkkojen siltojen ja

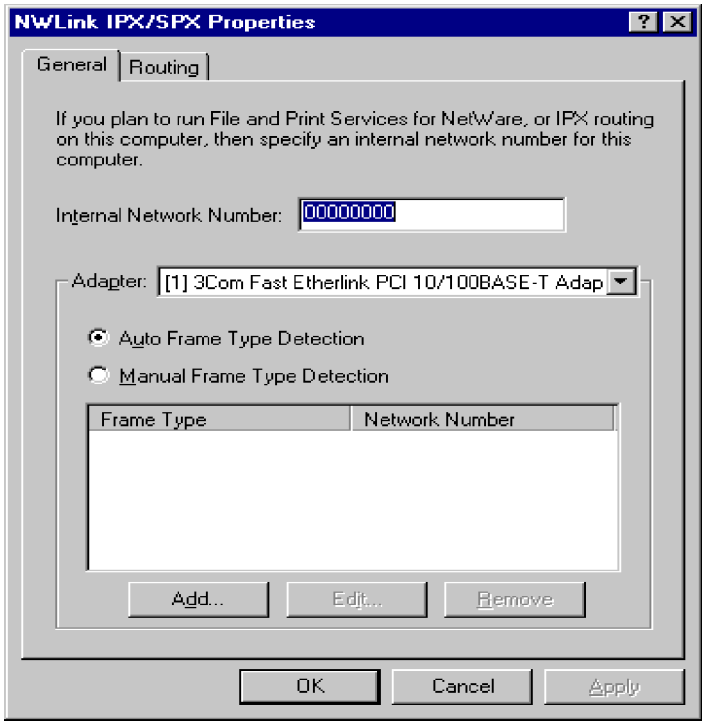
reitittimien välillä. Myös Windows NT:n **etäkäyttöpalvelu** (RAS) tukee PPP-protokollaa, ja sen asentaminen on edellytys PPP:n käytölle

- **Streams Environment** - STREAMS on alunperin **AT&T**:n kehittämä **Unix System V, Release 3.2**:een ja se kokoaa yhteen STREAMS-pohjaiset siirtoprotokollat. STREAMS mahdollistaa olemassaolevien STREAMS-pohjaisten komponenttien tuomisen Windows NT -maailmaan
- **TCP/IP Protocol** - **TCP/IP** on yleisesti reititinverkoissa - kuten laajat yritysverkot tai Internet - käytetty protokolla. Se on myös eniten konfigurointia vaativa protokolla.

Painikkeella **Ominaisuudet** (Properties) voit määritellä protokollan asetuksia. Konfiguraatio kannattaa tarkistaa **NWLink IPX/SPX Compatible Transport**- ja **TCP/IP-protokollista**.

NWLink IPX/SPX Compatible Transport

NWLink IPX/SPX Compatible Transportissa voit asettaa IPX/SPX:n **kehystyypin** ja **sisäisen verkko-osoitteen**. Nämä riippuvat NetWare-verkostasi. Tarvitset IPX/SPX:ää esimerkiksi, jos käytät NetWare-palvelinta NT-työasemasta **NetWare-asiakaspalvelulla** (Client Service for NetWare) tai olet perustanut palvelimeen **NetWare-yhdyskäytävän** (Gateway Service for NetWare).

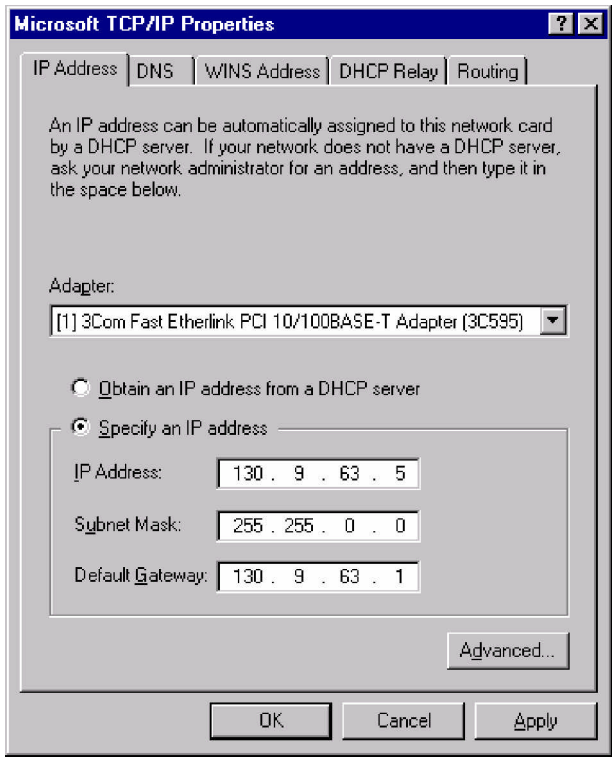


TCP/IP

TCP/IP-asetuksissa on neljä välilehteä, IP-osoite **IP Address**, **DNS**, WINS-osoite **WINS Address** ja reititys **Routing**.

IP Address-välilehdessä annetaan IP-osoite ja aliverkon maski eli peite. Nämä ovatkin ainoat pakolliset TCP/IP-asetukset.

Voit myös käyttää DHCP-palvelua hyväksesi valitsemalla **Obtain an IP address from DHCP server**, se hakee IP-osoitteen DHCP-palvelimesta. Yleensä näin ei tehdä palvelimien tapauksessa!


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
DHCP Relay
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] 3Com Fast Etherlink PCI 10/100BASE-T Adapter (3C595)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
130 . 9 . 63 . 5
Subnet Mask:
255 . 255 . 0 . 0
Default Gateway:
130 . 9 . 63 . 1
Advanced...
OK
Cancel
Apply

Asetukset ovat seuraavat:

- Valitse **Adapter**-luettelosta verkkokortti, jolle haluat määrittää IP-osoitteet; siinä on kaikki asennetut verkkokortit, joihin IP-protokolla on sidottu tässä työasemassa tai palvelimessa. Tee verkkoympäristösi mukaiset asetukset - jos et käytä DHCP-palvelua, anna IP-osoite kohtaan **IP Address** ja aliverkon peite kohtaan **Subnet Mask**. IP-osoite-ruudussa oleva arvo osoittaa paikallisen työaseman tai palvelimen IP-osoitteen; jos mikroon on asennettu useita verkkokortteja, arvo on **Adapter**-ruudusta valitun verkkokortin IP-osoite.

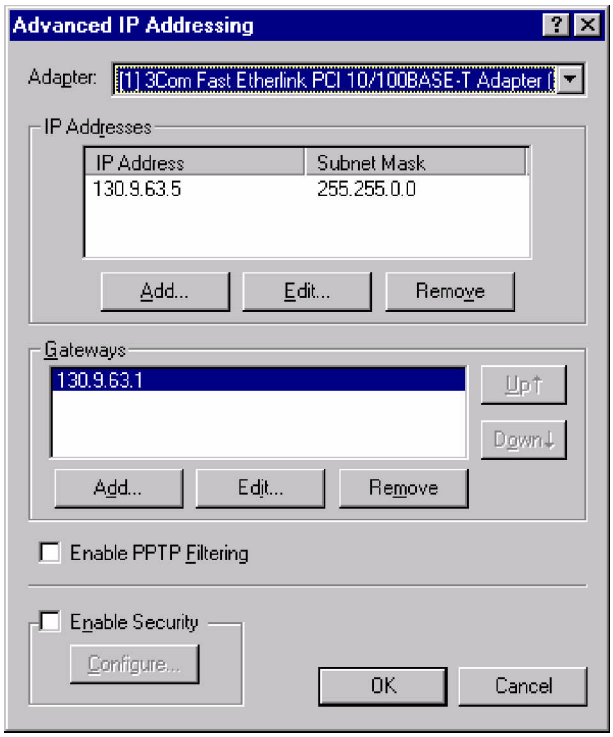
- **Subnet Mask** -ruudussa oleva arvo määrittelee valitun verkkokortin jäsenyyden verkossa ja isäntätunnuksen (*host*). Tämän arvon avulla järjestelmä jakaa IP-osoitteen isäntä- ja verkko-osoitteeksi.

- Anna **oletusyhdyskäytävä** kohtaan **Default Gateway** kullekin verkkosovittimelle oikea arvo, joka määrittää oletusyhdyskäytävän tai IP-reitittimen (*router*) IP-osoitteen, jota käytetään pakettien reitittämiseen toisiin verkkoihin tai aliverkkoihin. Tämän arvon tulisi olla jokin paikallisen yhdyskäytävän IP-osoite. Oletusyhdyskäytävän osoitetta tarvitaan verkoissa, jotka koostuvat **useista aliverkoista** tai ovat **yhteydessä toisiin verkkoihin**. Jos parametria ei ole annettu, **IP:n toiminta rajoittuu paikalliseen aliverkkoon**, ellei reittiä erikseen määritetä staattisesti TCP/IP:n **ROUTE**-komennolla.

Paina **Advanced**-painiketta, niin voit antaa lisäasetuksia:

- Voit lisätä verkkokorteillesi useitakin IP-osoitteita kohdassa **IP Address**

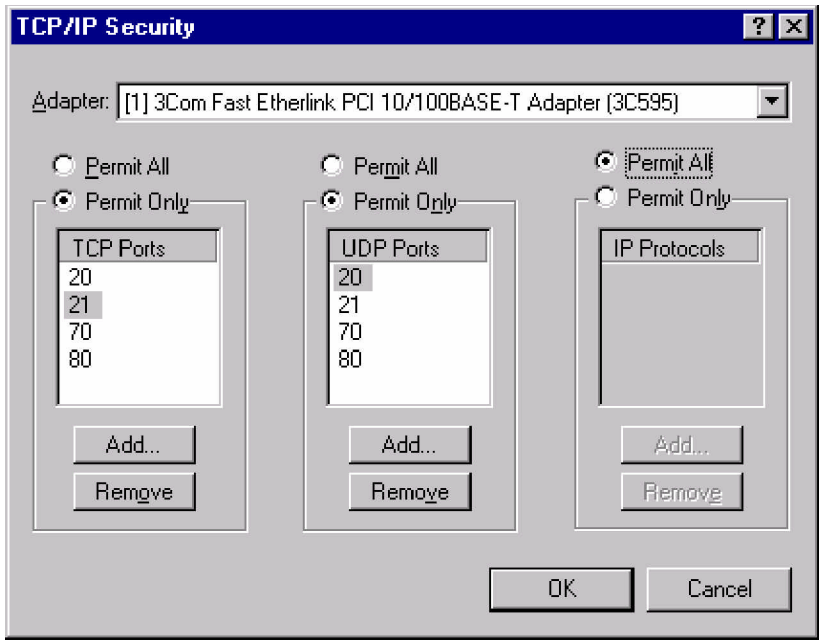
- Lisää myös aliverkon peite kohdassa **Subnet Mask** ja oletusyhdyskäytävä kohtaan **Default Gateway**. Tämä voi olla hyödyllistä yhdessä fyysisessä verkossa, jossa on kuitenkin useita loogisia IP-verkkoja.



- Voit ottaa käyttöön PPTP-suodatuksen valitsemalla **Enable PPTP Filtering**. PPTP (*Point-to-Point Tunneling*) muodostaa tunnelin, jonka sisälle paketoidaan RAS-yhteyden läpi lähetettävät PPP-paketit. Koska RAS tukee salakirjoitusta, siirrettävä data salakirjoitetaan käyttäen **RSA RC4** -menetelmää ja **40-bittistä avainta**, joka muodostetaan PPP-yhteydenmuodostuksessa RAS-asiakkaan ja Windows NT RAS-palvelimen välille. PPTP:tä voi käyttää esimerkiksi siten, että ensin otetaan PPP-yhteys Internet-yhteyden tarjoajaan, minkä jälkeen muodostetaan Internetin yli PPTP-yhteys omaan RAS-palvelimeen. PPTP käyttää **PAP** (*Password Authentication Protocol*)- ja **CHAP** (*Challenge Handshake Authentication Protocol*)-salakirjoitusalgoritmeja. PPTP voi kuljettaa myös IPX- ja NetBEUI -paketteja.

- Valinnalla **Enable Security** voit määritellä, mitä **TCP**- ja **UCP**-portteja sekä **IP-protokollia** työaseman valittu verkkoliitäntä käsittelee. Asetukset ovat yhdensuuntaisia, lähteviin paketteihin asetukset eivät vaikuta.

Mahdollisuus määritellä työaseman/palvelimen käyttämät portit per verkkokortti on varsin vahva ominaisuus, koska mikro voidaan varustaa kahdella verkkokortilla; toinen verkkokortti on kytketty avoimeen verkkoon ja toinen sallii esimerkiksi vain **Internet Information Server**-palvelimen käyttämät portit: toinen verkkokortti on kytketty sisäiseen suojattuun verkkoon. Se sallii kaikki tarvittavat portit ja protokollat.



Sallitut portit ovat tässä esimerkissä:

20/tcp, udp	ftp-data, File Transfer
21/tcp, udp	ftp, File Transfer (Control)
70/tcp, udp	Gopher
80/tcp, udp	HTTP, WWW-palvelin

Oleellisia portteja **NetBIOS-palveluiden** (*NetBIOS Over TCP/IP*, **NetBT**) kannalta ovat seuraavat:

Protokolla	**Portti**	**Merkitys**
UDP	53	DNS-nimikysely
UDP	137	NetBIOS-nimipalvelu
UDP	138	Tietosähkepalvelut
TCP	139	Yhteyspalvelut

Jos kiellät näiden porttien käytön ja TCP/IP on ainoa protokolla, seurauksena saattaa olla esimerkiksi verkkoonkirjautumisen tai verkkoresurssien käytön epäonnistuminen.

Lisäksi **DHCP** käyttää UDP-portteja **67** ja **68**.

Sallitut protokollat annetaan **numerolla**: esimerkiksi

Protokolla	Numero	Kuvaus
IP	0	Internet protocol
ICMP	1	Internet control message protocol
GGP	3	Gateway-gateway protocol
TCP	6	Transmission control protocol
EGP	8	Exterior gateway protocol
PUP	12	PARC universal packet protocol
UDP	17	User datagram protocol
HMP	20	Host monitoring protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	“Reliable datagram" protocol
PPTP	5678	Point-to-point Tunneling Protocol
RVD	66	MIT remote virtual disk

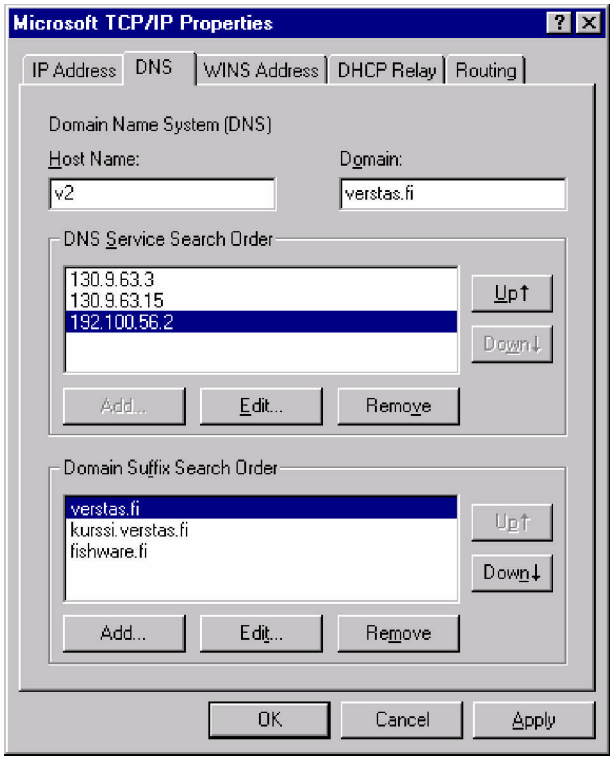
Seuraavana on **lyhyt lista** ns. **Tunnetuista TCP-porteista** (*Well Known Port Numbers*, **RFC 1700**, ks. **http://ds.internic.net/std/std2.txt**).

Lisää löydät **WINNT\System32\Drivers\Etc**-hakemiston **Services**-tiedostosta.

Lisää tietoja löytyy **Winnt\System32\Drivers\Etc**-hakemiston tiedostoissa SERVICES, PROTOCOL ja NETWORKS.

Portti	Palvelu	Kuvaus
1	TCPMUX	TCP Port Service Multiplexer
5	RJE	Remote Job Entry
20	FTP-DATA	File Transfer Protocol - Data
21	FTP	File Transfer Protocol - Control
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer Protocol
42	NAMESERV	Host Name Server
49	LOGIN	Login Host Protocol
53	DOMAIN	Domain Name System
69	TFTP	Trivial File Transfer Protocol
70	GOPHER	Gopher
80	HTTP	HTTP
103	X400	X.400
110	POP3	Post Office Protocol version 3
137	NETBIOS-NS	NetBIOS Name Service
139	NETBIOS-DG	NetBIOS Datagram Service
150	NETBIOS-SS	NetBIOS Session Service
156	SQLSRV	SQL Server
179	BGP	Border Gateway Protocol

DNS-välilehdellä määritellään DNS:n asetukset:

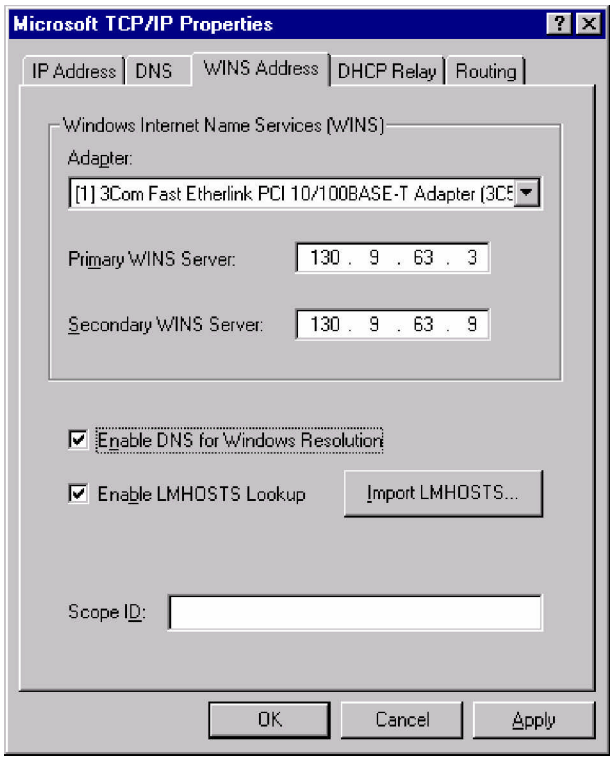


- Voit määritellä **Host** -kohtaan oman palvelimen nimen ja **Domain** -kohtaan organisaatiosi (tavallisesti **organisaatio.tarkennin**) - tällä ei ole mitään tekemistä Windows NT -toimialueen kanssa!

- **DNS Service Search Order** -listaan voit antaa hakujärjestyksen verkon DNS-palvelimille. Vain jos listan ensimmäinen ei vastaa, kysely siirtyy listan seuraavalle DNS-palvelimelle

- Domain Suffix Search Order -listaan voit lisätä muita toimialue (domain)-nimiä, jolloin voit määritellä toimialueen jälkiliitteen etsintäjärjestyksen. Tämä tarkoittaa sitä, että esimerkiksi etsittäessä **V1** nimistä isäntäkonetta ensin etsitään **V1.VERSTAS.FI**

WINS Address -välilehdessä määritellään NetBIOS-nimiselvitysmenetelmät.



Asetukset ovat:

- Jos verkkoon on asennettu **WINS**-palvelimia ja haluat selvittää palvelimien tai työasemien nimiä käyttämällä WINS-palvelua, kirjoita ensisijaisten (**Primary WINS Server**) ja toissijaisten WINS-palvelinten (**Secondary WINS Server**) a.o. ruutuihin IP-osoitteet. WINS-palvelimien tiedot voidaan saada myös DHCP:n avulla. Jos WINS-palvelimille ei määritetä osoitteita, Windows NT käyttää nimikyselyjen **yleislähetyksiä** (*broadcasts*) ja paikallista työaseman tai palvelimen **LMHOSTS**-tiedostoa selvittäessään IP-osoitetta nimen perusteella. Tiedosto sijaitsee NT:n järjestelmähakemiston alla **SYSTEM32\DRIVERS\ETC**-hakemistossa. Yleislähetyksiin (broadcast) perustuvaa nimiselvitystä voi käyttää vain paikallisessa verkossa.

- Jos haluat käyttää DNS:ää Windows-verkkosovelluksissa, valitse **Enable DNS for Windows Name Resolution**. Tällöin DNS-palvelimessa tulee olla määriteltyinä myös Windows NT -palvelinten tiedot. Tällöin myös käytetään tarvittaessa **HOSTS**-tiedostoa

- Jos haluat käyttää **LMHOSTS**-tiedostoa verkon laitteiden NetBIOS-nimien selvittämiseen, valitse **Enable LMHOSTS Lookup**. **Import**-painikkeella haetaan LMHOSTS-tiedosto, jolloin pystyt asentamaan esimerkiksi **varaohjauskoneen** (*Backup Domain Controller*) reititinverkossa

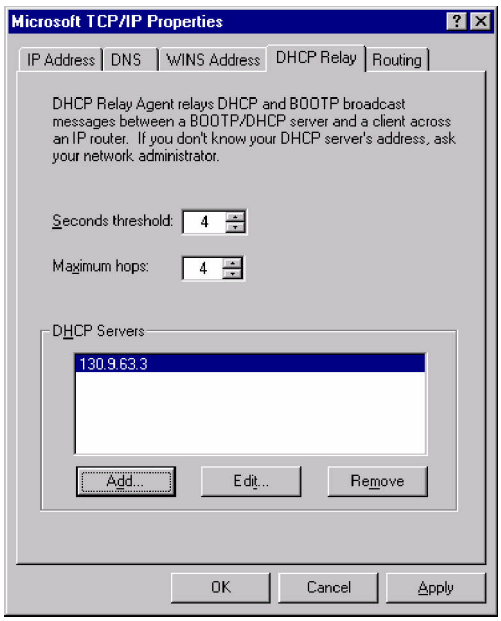
- Aluetunnus **Scope ID** tarvitaan joissakin sovelluksissa jotka käyttävät NetBIOS:ia TCP/IP:n päällä (*NetBIOS over TCP/IP*). Tällöin sen on oltava sama kaikissa keskenään kommunikoivissa koneissa. Oletus on tyhjä.

Tyypillisesti järjestys nimien ratkomisessa on ensin **WINS** tai **broadcast-sanomat**, sitten **LMHOSTS** ja lopuksi **DNS**. **LMHOSTS**-tiedoston pitää sijaita Windows NT:n **SYSTEM32\DRIVERS\ETC**-hakemistossa; se on ASCII-tiedosto ja asetusrivit ovat siinä muotoa:

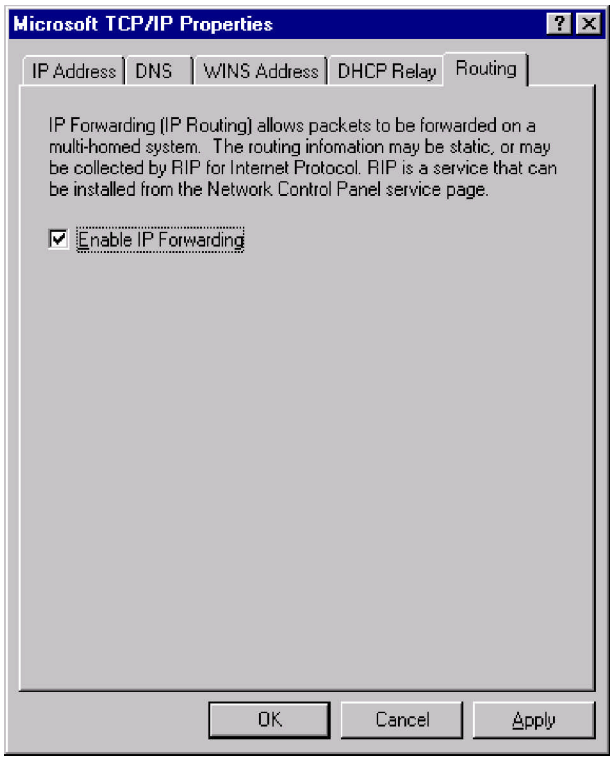
```
193.88.121.65   V1    #PRE     #DOM:VERSTAS   #VERSTAS Primary Domain Controller
```

eli ensin IP-osoite, sitten NetBIOS-nimi, sitten optiot (esimerkiksi latausmenettely) ja muut määrittelyt.

DHCP Relay -välilehdessä määritellään palvelimen toimiminen **DHCP**- ja **BOOTP**-kyselyjen välittäjänä. Määrittele kyselyjen ohjauksessa tarvittavat vasteajat ja varsinaisten DHCP-palvelinten osoitteet kohdassa **DHCP Servers**.



Routing-välilehdessä voit ottaa **staattisen IP-reitityksen** käyttöön valitsemalla **Enable IP Forwarding**, jolloin palvelin voi toimia reitittimenä verkon muiden staattisten reitittimien ohella. Vaihtoehto kannattaa valita, jos palvelimessa on vähintään kaksi verkkokorttia ja verkko käyttää staattista reititystä **ROUTE**-komennon avulla tai palvelimessa on käytössä kaksi IP-osoitetta.



RIP-reititysprotokolla (*Routing Information Protocol*) sopii hyvin pieniin verkkoihin ja se on lisäksi usein ainoa vaihtoehto, jos verkossa on useiden eri valmistajien reitittimiä. RIP käyttää eri verkkojen etäisyyden mittana kyseisellä reitillä olevien reitittimien lukumäärää, jolloin paras reitti kahden solmun välillä on vähiten reitittimiä käsittävä. Muita reititysprotokollia ovat **Ciscon** kehittämä ja käyttämä **IGRP** (*InterGateway Routing Protocol*) ja **OSPF** (*Open Shortest Path First*) sekä **OSI**:n standardoima **IS-IS** (*Integrated IS-IS* tai *Dual IS-IS*) OSI-verkkoja varten.

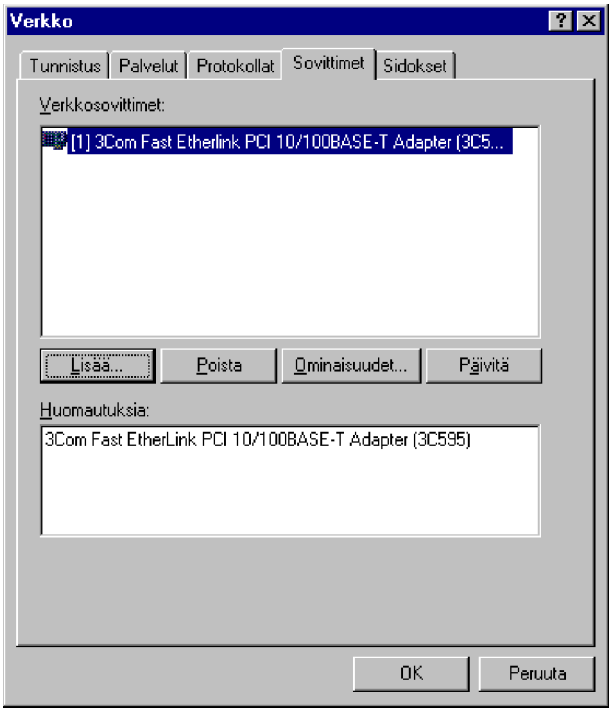
Kun TCP/IP on asennettu, NT:n hakemistossa **\SYSTEM32\DRIVERS \ETC** on mm. **HOSTS**-, **NETWORKS**-, **PROTOCOLS**-, **QUOTES**- ja **SERVICES**-oletustiedostot sekä mallitiedosto **LMHOSTS.SAM**, jossa selitetään **LMHOSTS**-tiedoston muoto.

NT-työaseman tai -palvelimen TCP/IP-asetukset näet komennolla **IPCONFIG**. Lisävalitsimella **/ALL** näet yksityiskohtaiset tiedot:

```
Windows NT IP Configuration

  Host Name . . . . . . . . . . . . . . . . .  pc-jki1.fishware.fi
  DNS Servers . . . . . . . . . . . . . . . .  130.9.32.2
                                               130.9.30.2
  Node Type . . . . . . . . . . . . . . . . .  Hybrid
  NetBIOS Scope ID. . . . . . . . . . . . . .
  IP Routing Enabled. . . . . . . . . . . . .  No
  WINS Proxy Enabled. . . . . . . . . . . . .  No
  NetBIOS Resolution Uses DNS . . .  Yes

Ethernet adapter CpqNF31:
  Description . . . . . . . . . . . . . . . .  Compaq NetFlex-3 Driver, Version 1.75
  Physical Address. . . . . . . . . . . . . .  00-80-5F-31-7A-82
  DHCP Enabled. . . . . . . . . . . . . . . .  Yes
  IP Address. . . . . . . . . . . . . . . . .  130.9.63.176
  Subnet Mask . . . . . . . . . . . . . . . .  255.255.0.0
  Default Gateway . . . . . . . . . . . .. ..  130.9.63.1
  DHCP Server . . . . . . . . . . . . . . ..  130.9.63.76
  Primary WINS Server . . . . . . . . . .  130.9.63.3
  Lease Obtained. . . . . . . . . . . . . . .  Thursday, June 26, 1997 7:45:00 AM
  Lease Expires . . . . . . . . . . . . . . .  Thursday, July 03, 1997 7:45:00 AM
```

Adapters

Verkkokortin (Adapter) avulla palvelin liitetään lähiverkon kaapelointiin.



Tee valinta käyttämäsi verkkokortin mukaan. Asennuksen jälkeen painamalla **Properties** voit *mahdollisesti* tutkia verkkokortin asetuksia. Verkkokortista riippuen voit esimerkiksi määrittää käytettävän liitäntämenetelmän eli verkkokaapelin tyypin (**Connector Type**). Valintoja voivat olla Ethernet-kaapelointia käytettäessä **parikaapeli** (Twisted Pair) tai **koaksiaalikaapeli** (BNC). Lisäksi voit ehkä valita mikron väylän, jota verkkokortti käyttää (ISA, PCI, VESA jne).

AUI/DIX-liitintä käytetään kytkettäessä mikron ns. **Paksuun Ethernet**-kaapeliin (ThickNet, 10Base5). Jos käytät esimerkiksi parikaapeliliitännättömässä verkkokortissa sovitinkappaletta liittämään palvelimen parikaapeliin - liität sovitinkappaleen **AUI/DIX**-liittimeen - muista myös valita liittimeksi **AUI/DIX**!

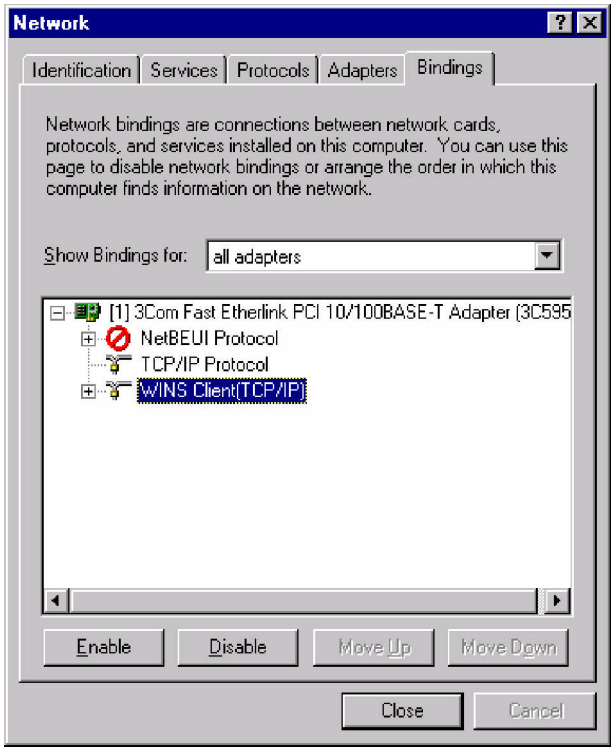
Nykyisissä palvelimissa yhä useammin verkkoliitännän tunnistus tapahtuu automaattisesti (esimerkiksi Compaqit).

Bindings

Bindings määrittelee sidokset verkkokomponentteihin, jotka käyttävät kyseistä protokollaa.

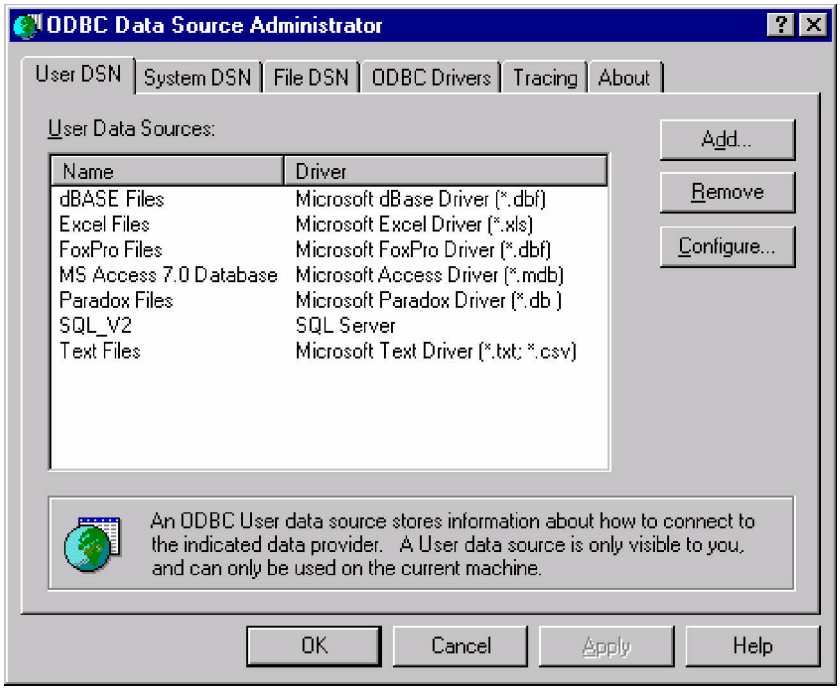
Voit valita halutun sidoksen valitsemalla **Show Bindings for**-luettelosta kaikki palvelut **all services**, kaikki protokollat **all protocols**, tai kaikki sovittimet **all adapters**. Halutun sidoksen voit ottaa käyttöön (**Enable**) tai poistaa käytöstä (**Disable**). Voit myös muuttaa sidosten käyttöjärjestystä ja siten muuttaa protokollien oletusjärjestystä.

Diagnostiikassa tätä menetelmää voi käyttää näppärästi hyväksi tutkittaessa saadaanko tietty palvelu tai resurssi käyttöön sulkemalla eri sidoksia. Tällöin ei kuitenkaan tarvitse poistaa kyseistä palvelua tai protokollaa.



ODBC

ODBC-asetuksilla (*Open DataBase Connectivity*) voidaan määritellä paikallisten sovellusten käyttämät tietokannat ja tiedostomuodot. Asetukset riippuvat asennetuista sovellutuksista ja tietokannoista.



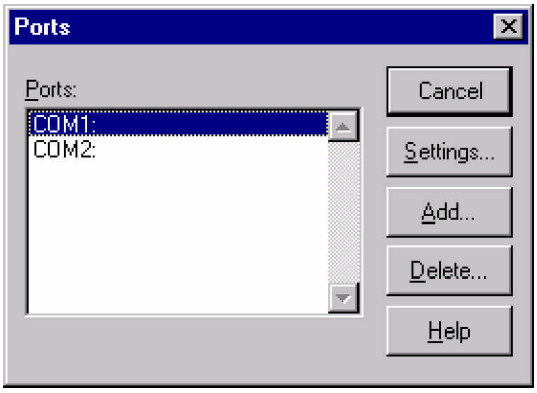
Ports

Sarjaliitäntäportin valinta ja asetukset

Ports mahdollistaa sarjaliikenneporttien COM1…COM256-määrittelyt. Niitä tarvitaan tietoliikenneohjelmissa, jotka osaavat suoraan asettaa käyttöön halutut sarjaliikenneportin asetukset.

COM5…COM256 tulevat kyseeseen, jos esimerkiksi **Windows NT -palvelin** tarjoaa etäkäyttöpalvelua (*Remote Access Service*)-palvelua

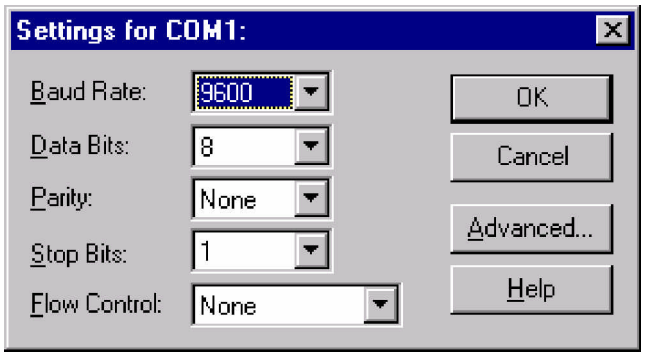
useille samanaikaisille käyttäjille. Tällöin toki mikroon tarvitaan lisäsarjaportit mahdollistava lisäkortti, esimerkiksi **DigiBoard EPC**.



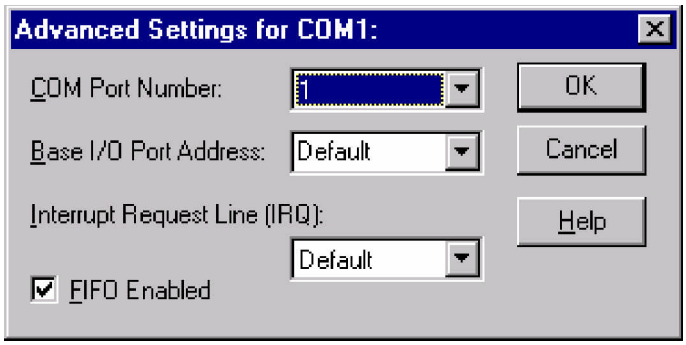
Sarjaportin lisäasetusten määrittäminen tehdään valitsemalla sarjaportille I/O-portin perusosoite ja keskeytys (IRQ) lisäasetusten **Advanced Settings**-valintaikkunassa. Lisäksi voit vaihtaa portin numeron ja ottaa käyttöön suorituskykyä parantavan saapuvien tietojen puskuroinnin (FIFO, *First In - First Out*).

Sarjaportin lisäasetusten määrittäminen tehdään seuraavasti:

1) Valitse **Ports**-kuvake ja kaksoisnapsauta haluamaasi porttia tai valitse ensin portti ja sitten **Settings**-painike



2) Valitse **Advanced**-painike:



- Muuta I/O-portin perusosoitetta, jos sarjaporttiin liitetty laite käyttää muita kuin Windows NT:n käyttämiä arvoja

- Jos mikrosi ei voi käyttää samanaikaisesti portteja COM1 ja COM3 tai COM2 ja COM4, mutta haluat käyttää näitä portteja, määritä **eri** IRQ-arvo kullekin sarjaportille

- Vaihda portin numero; vaihda esimerkiksi portin COM3 numeroksi COM253

- Ota saapuvien tietojen puskurointi käyttöön valitsemalla FIFO käyttöön (**FIFO Enabled**); se laajentaa uudempien COM-porttien toimintoja

3) Valitse **OK**; muutokset tulevat voimaan vasta, kun käynnistät NT:n uudelleen valitsemalla **Restart Now**.

Printers

Kirjoittimien asetukset valitaan Printers-kuvakkeella. Voit lisätä kirjoittimen tai muuttaa niiden oletusasetuksia.

Oletusasetusten muutos onnistuu yleensä myös suoraan sovelluksista tai kirjoitinkohtaisesta hiiren pikavalikosta valitsemalla **Properties**. Ne ovat aina kirjoitinkohtaisia eli saattavat vaihdella hyvinkin paljon riippuen käyttämästäsi kirjoittimesta: väri-/mustavalkokirjoitin, mustesuihku- tai laserkirjoitin ja niin edelleen. Esimerkiksi tavallisella matriisikirjoittimella on vain muutama asetus.

Kirjoittimen asetuksissa käytettävissä olevat välilehdet ovat seuraavat:

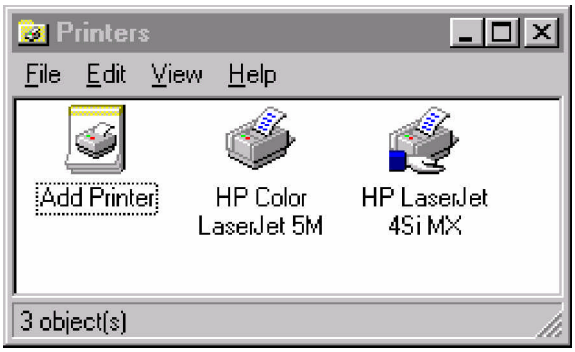
- **General** - yleiset asetukset
- **Ports** - käytetty kirjoitinportti
- **Scheduling** - tulostuksen ajoitus
- **Sharing** - kirjoittimen jakaminen verkkoon (ks. **Luku 7**)
- **Security** - kirjoittimen käytön suojaukset (ks. **Luku 7**)
- **Device Settings** - muisti- ja arkinsyöttölokeron asetukset.

Voit myös avata **Printers**-ikkunan ja valittuasi halutun kirjoittimen käsitellä sen asetuksia **File**-valikosta **Properties**-valinnalla. Kirjoittimia ja tulostusta **verkossa** on käsitelty luvussa **7.**

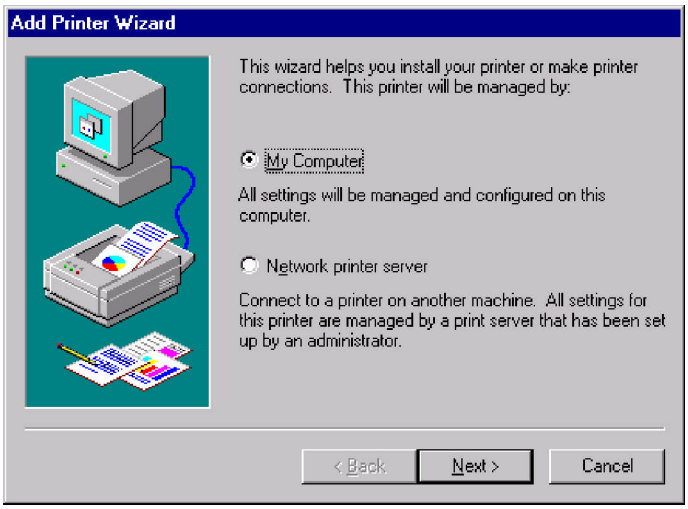
Add printer

Mikroon kytketyn kirjoittimen lisääminen tehdään seuraavasti (verkkokirjoittimet - katso luku **7**):

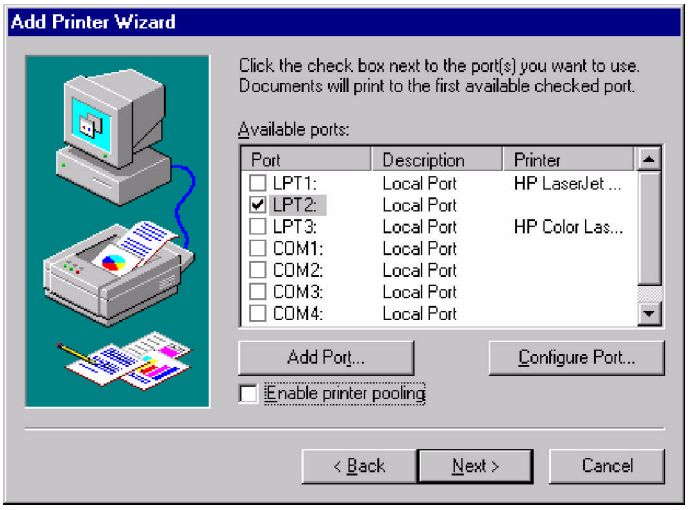
1) Avaa Ohjauspaneelin **Printers** ja napauta **Add Printer**-kuvaketta



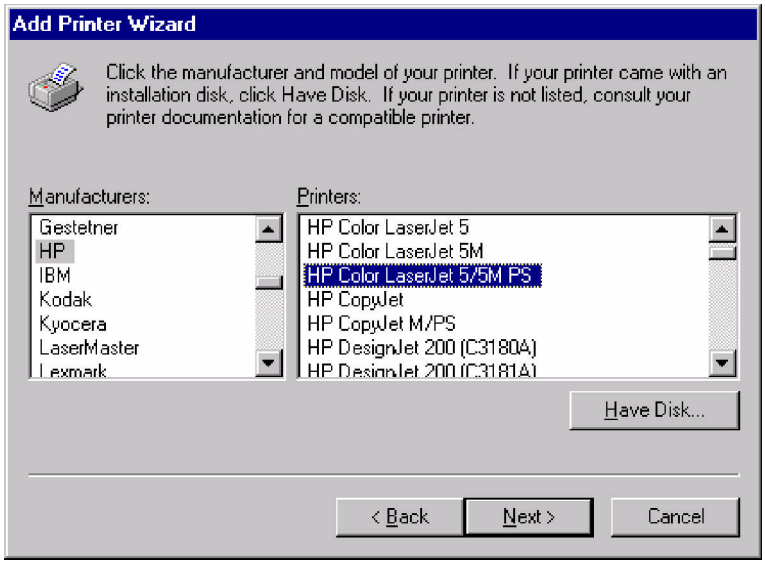
2) Tällöin avautuu uuden kirjoittimen asennusvelho, joka kyselee asennettavan kirjoittimen tiedot. Valitse kirjoittimen kytkentä omaan tietokoneeseen (**My Computer**) ja paina **Next**



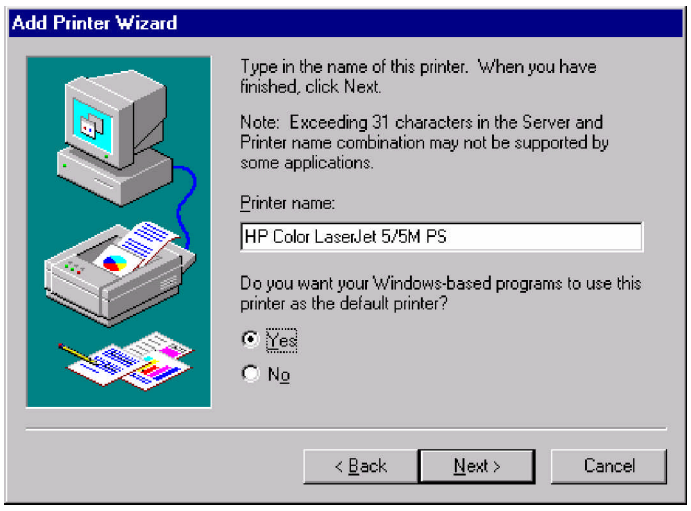
3) Valitse tulostusliitäntä tai tulostus tiedostoon (**FILE:**). Suositeltavin on rinnakkaisportti LPT1, LPT2 tai LPT3. Tavallisesti mikroista löytyy ainakin **LPT1**. Valinnalla **Enable printer pooling** voitaisiin määritellä useampi fyysinen kirjoitin yhteen tulostusjonoon (ks. myös **Luku 7**). Paina **Next**



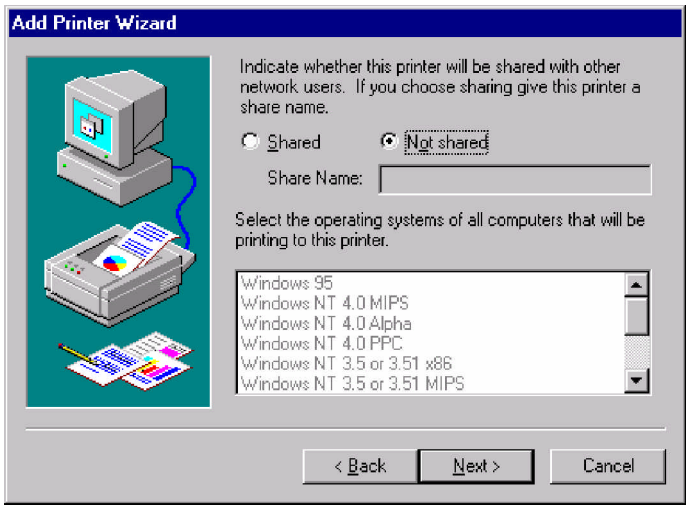
4) Anna kirjoittimen tyyppi. Jos haluttua ei löydy tai jos haluat asentaa päivitetyn kirjoitinohjaimen (*driver*), valitse **Have Disk**. Muuten paina **Next**



5) Voit myös saada kysymyksen, käytetäänkö nykyistä kirjoitinajuria vai asennetaanko uusi. Seuraavaksi voit antaa kirjoittimen nimen (näkyy mm. kirjoittimen kuvakkeessa) sekä valita, käytetäänkö kirjoitinta oletuskirjoittimena **Default printer**. Paina **Next**



6) Seuraavaksi kysytään kirjoittimen jakamista, valitaan ei jaettu **Not shared** (verkkokirjoittimet - katso luku **7**):



7) Seuraavaksi kysytään, tulostetaanko testisivu. Oletus on, että tulostetaan. Tulostusta kannattaakin kokeilla jo nyt!

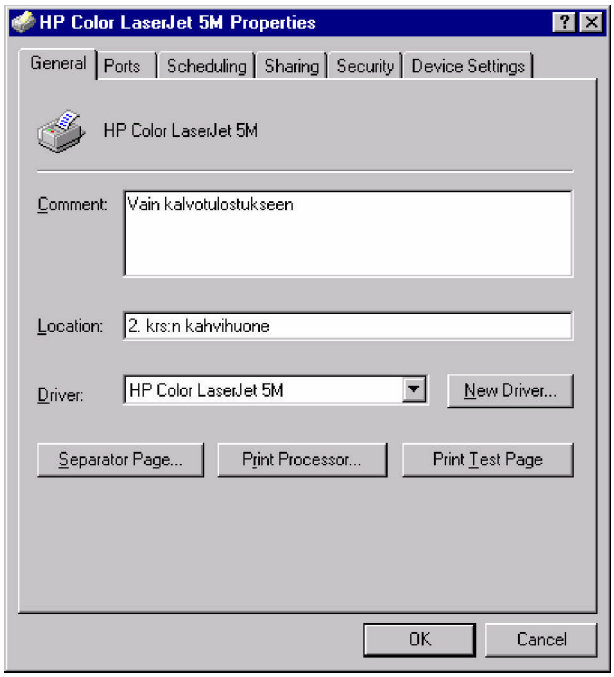
8) Tämän jälkeen asennetaan tarvittavat kirjoitinajurit. Muuttaessasi Ohjauspaneelin kautta laitteistoasetuksia saatat tarvita Windows NT:n CD-ROM:ia tai verkkoyhteyttä hakemistoon, missä asennustiedostot sijaitsevat. Yleensä Windows NT osaa itse hakea tarvittavat

tiedostot, mutta tarvittaessa se osaa myös kysyä, mistä asennustiedostot löytyvät. Voit antaa sijainnin myös UNC-nimenä, esimerkiksi **\\PALVELIN\PCTUKI\NT4SRV\i386**

9) ... ja lopuksi odotetaan vastausta kysymykseen, tulostuiko testisivu oikein. Jos tulostui, kirjoitin on valmis käyttöön. Jos tiedät, että kirjoitin ei ole päällä tai verkkoyhteys ei ole kytkettynä, ei testisivua kannata luonnollisestikaan tulostaa.

General

Voit avata **Printers**-ikkunan ja valittuasi halutun kirjoittimen käsitellä sen asetuksia **File**-valikosta **Properties**-valinnalla. Saman voi tehdä hiiren pikavalikosta.



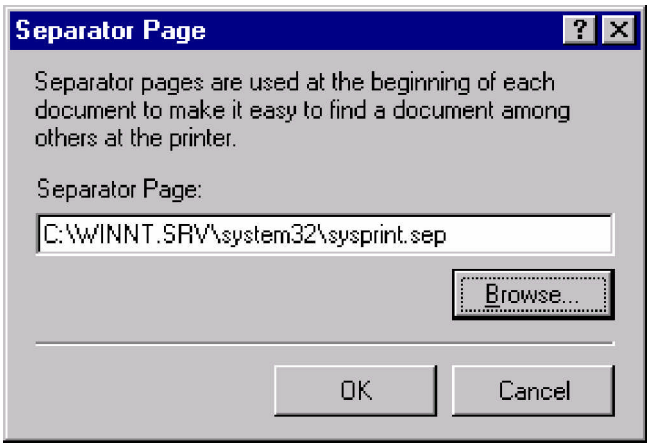
General - välilehti sisältää yleiset asetukset:

- **Comment** - kirjoita kuvaus kirjoittimesta
- **Location** on kirjoittimen fyysisen sijaintipaikan kuvaus. Sen avulla muut verkkokäyttäjät tietävät, mistä etsiä tulostettuja töitä

- **Driver** on kirjoitinohjain - voit valita minkä tahansa **asennetun** kirjoitinohjaimen

- **Separator Page** - jos **erotinsivu** on valittu käyttöön, se tulostetaan aina tulostustöiden väliin; se on kuitenkin valittavissa käyttöön vain paikallisessa, suoraan mikroon kytketyssä kirjoittimessa; verkkokirjoittimet käyttävät tavallisesti omia, palvelimissa asetettuja erotinsivujaan. Windows NT:n mukana toimitetaan seuraavat erotintiedostot:

  - **SYSPRINT.SEP** - tulostaa erotinsivun jokaisen tulosteen alkuun
  - **PCL.SEP** - vaihtaa kirjoittimen PCL-moodiin; tiedostoa voi muokata
  - **PSCRIPT.SEP** - vaihtaa kirjoittimen PostScript-moodiin; tiedostoa voi muokata.



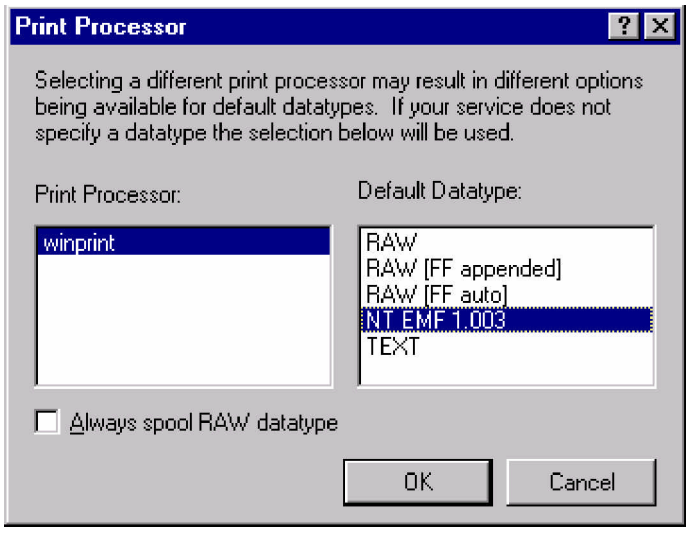
Erotinsivun määrittäminen tehdään etsimällä halutun erotintiedoston nimi ja polku **Separator Page**-ruutuun. Tarvittaessa voit valita vieressä olevan selauspainikkeen ja etsiä halutun tiedoston.

Erotinsivuilla voit käyttää seuraavia ohjauskoodeja:

Ohjauskoodi	**Merkitys**
@N	Käyttäjätunnuksen tulostaminen
@I	Työn numeron tulostaminen
@D	Päiväys (Ohjauspaneelin maa-asetusten mukaan)
@T	Kellonaika (Ohjauspaneelin maa-asetusten mukaan)
@L	Tulostaa kaikki merkit seuraavaan ohjauskoodiin saakka tai @W:llä määriteltyyn sivun leveyteen saakka
@F*tiedosto*	Tulostaa *tiedoston* sisällön
@H*nn*	Tulostaa *nn:llä* määritellyn heksadesimaalikoodin (esimerkiksi @H1B on *escape* (1B heksadesimaalina, 27 desimaalina)
@W*nnn*	Sivun leveys (oletus 80, maksimi 256)
@B@S	Normaalileveyksiset palkkimerkit käytössä
@B@M	Tuplaleveyksiset palkkimerkit käytössä
@U	Kytkee pois palkkimerkit
@*n*	Ohittaa *n* riviä
@E	Sivun syöttö

Jos NT-kone jakaa kirjoitintaan (asetetaan **Sharing**-välilehdessä), niin silloin erotinsivu voi olla hyvä ottaa käyttöön erottelemaan käyttäjien tulostustyöt toisistaan.

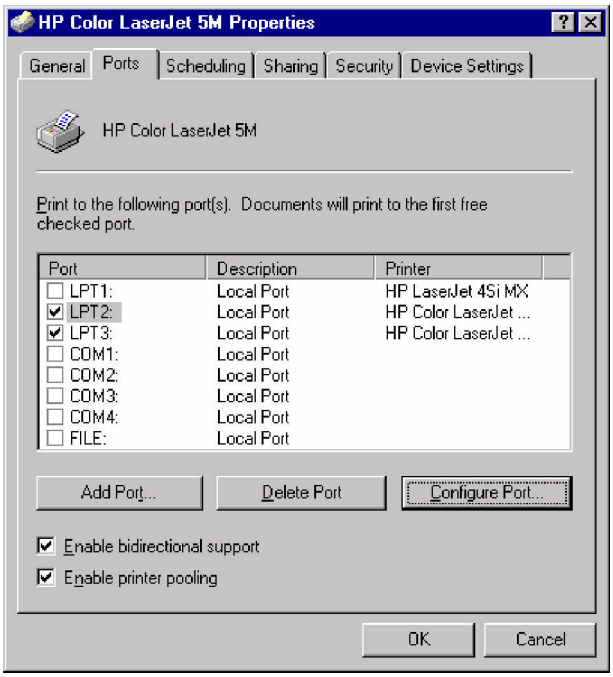
- **Print Processor** voidaan muuttaa esimerkiksi tulostustöiden sivunsyöttöä; **RAW (FF appended)** lisää sivunsyötön ja **RAW (FF auto)** lisää sen tarvittaessa. **RAW** lähettää tulostustyön sellaisenaan kirjoittimelle. **NT EMF** on Windows NT:n **GDI**:n tulostus, jonka kyseisen kirjoittimen ohjain konvertoi kirjoittimelle sopivaksi - tällöin tulostus on kohtuullisen nopeaa. **TEXT**-valinnalla voidaan tulostaa ASCII-tekstiä **PostScript**-kirjoittimelle.



- Lisäksi on mahdollisuus tulostaa testisivu valinnalla **Print Test Page**.

Ports

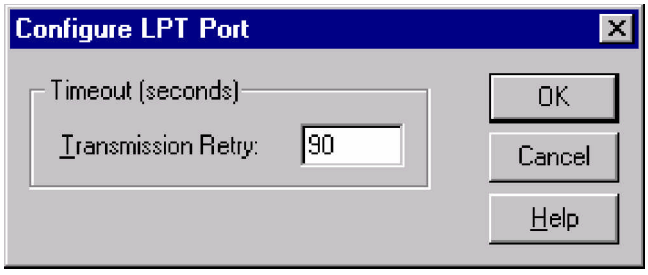
Ports määrittelee käytetyn kirjoitinportin.



- **Add port**-valinnalla voidaan lisätä portti (tavallisesti verkkokirjoitin - tällöin tulostus voidaan uudelleenohjata verkon kirjoittimelle)

- **Delete port**-valinta poistaa portin

- **Configure Port**-valinnalla voit ohjata rinnakkaisporttien aikakatkaisua eli aikaa, jonka kuluttua tulostuspalvelu päättää, että kirjoitin ei vastaa. Asetus vaikuttaa **valittuun kirjoittimeen** ja **kaikkiin samaa ohjainta** käyttäviin **paikallisiin kirjoittimiin**. Asetus **Transmission Retry** määrittää ajan, joka odotetaan ennen seuraavaa tulostamisyritystä; anna aika sekunteina. Valitse lopuksi **OK**

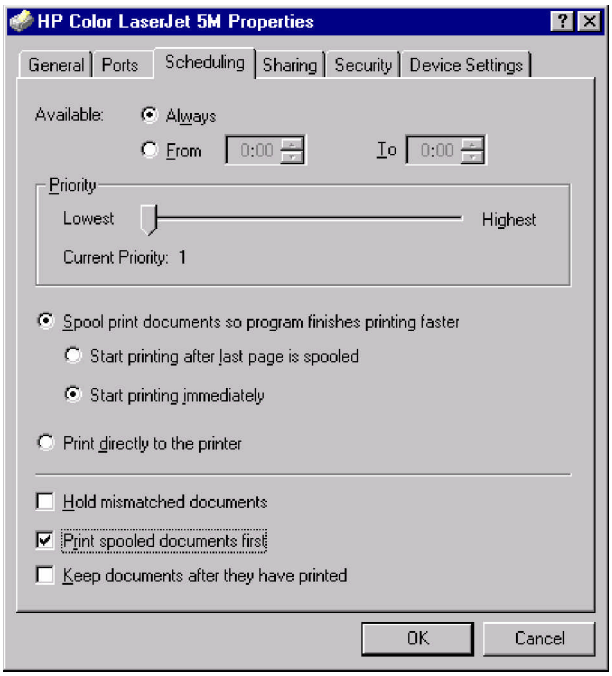


- **Enable bidirectional support** mahdollistaa kaksisuuntaisuustuen kirjoittimelle; tällöin kirjoitin voi esimerkiksi välittää tilatietojaan. Kirjoittimen ja mikron on tuettava kaksisuuntaisuutta

- **Enable printer pooling** mahdollistaa useamman fyysisen samanlaisen kirjoittimen kytkemisen yhteen loogiseen kirjoittimeen, ts. kirjoitinohjaimeen ja tulostusjonoon.

Scheduling

Scheduling määrittelee tulostuksen ajoituksen.



Tulostustöille voit antaa erilaisia asetuksia tarpeen mukaan. Näitä ovat mm. seuraavat:

- **Available** määrittelee käytettävyysajan, jolloin kirjoitin tulostaa sille lähetetyt työt. Töitä voi lähettää kirjoittimelle milloin tahansa, mutta kirjoitin tulostaa ne **vain annettuna ajanjaksona**. Voit esimerkiksi luoda kaksi kirjoitinta yhdelle fyysiselle kirjoittimelle ja rajoittaa toisen kirjoittimen tulostamisen vain päivän ja toisen vain yön ajaksi; yöllä voidaan tulostaa esimerkiksi useam-

pi satasivuisia raportteja jne. suuria ja ehkä vähemmän kiireellisiä töitä. Kiireelliset työt tulostetaan päivän aikana toisella kirjoittimella

- **Priority** -prioriteettimäärityksen avulla voit ohjata, mitkä työt kirjoitin tulostaa ensin. Jos luot kaksi kirjoitinta samalle fyysiselle kirjoittimelle ja määrität niille eri prioriteetin, fyysinen kirjoitin tulostaa aina ensin ne tulostustyöt, jotka on lähetetty **suuremman prioriteetin** kirjoittimelle

- Voit ohjata tapaa, jolla tulostuspalvelu lähettää työt kirjoittimelle kahdella valinnalla:

  - **Spool print documents so program finishes printing faster** - oletuksena tulostustyö tallennetaan ensin kiintolevylle, josta taustatulostin lähettää sen sitten kirjoittimelle. Tällöin sovellus on heti käytettävissä, kun työ on tallennettu kiintolevylle odottamaan taustatulostuksen päättymistä. Valinnat ovat **Start printing after last page is spooled**, jolloin odotetaan **koko työn** saapumista tulostusjonoon **ennen** tulostuksen aloittamista tai **Start printing immediately**, jolloin tulostus alkaa välittömästi

  - **Print directly to the printer** - jos haluat ohittaa tämän taustatulostusjonon käytön, voit tulostaa suoraan kirjoittimelle (**Print directly to the printer**); tällöin voit kuitenkin jatkaa sovelluksen käyttämistä vasta, kun tulostaminen sovelluksesta on päättynyt. Jaettu kirjoitin ei voi tyypillisesti käyttää tätä toimintoa; jos teet valinnan se poistetaan automaattisesti.

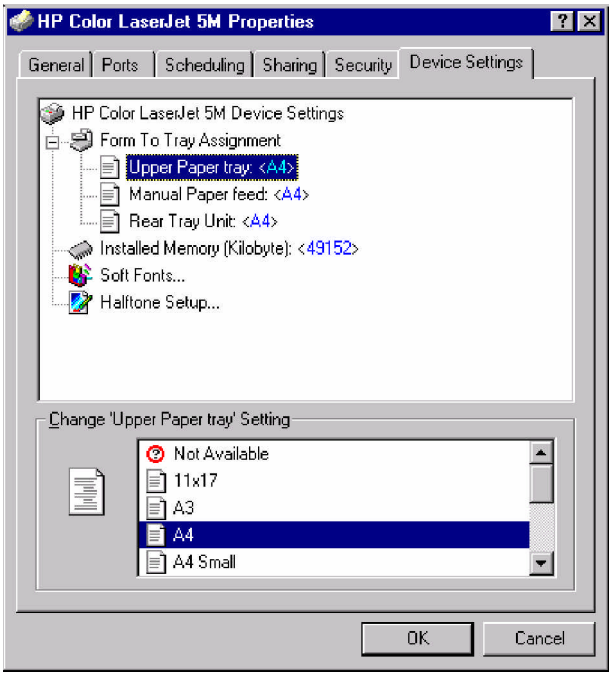
- **Hold Mismatched Documents** tarkistaa tulostustyön ja kirjoittimen asetukset; jos asetukset eivät täsmää, työ jää tulostusjonoon

- **Print spooled documents first** tulostaa jo taustatulostetut työt ennen osittain taustatulostettuja, **vaikka niillä olisikin korkeampi prioriteetti**

- **Keep documents after they have printed** jättää työn tulostusta ohjaavan NT-koneen levylle, jolloin tulostustyön voi toistaa ilman tulostuksen ajamista sovelluksesta.

Device Settings

Device Settings -laiteasetukset ovat kirjoitinkohtaisia. Tyypillisesti muisti- ja arkinsyöttölokeron asetukset voidaan määritellä lähes jokaiselle kirjoitimelle.



SCSI Adapters

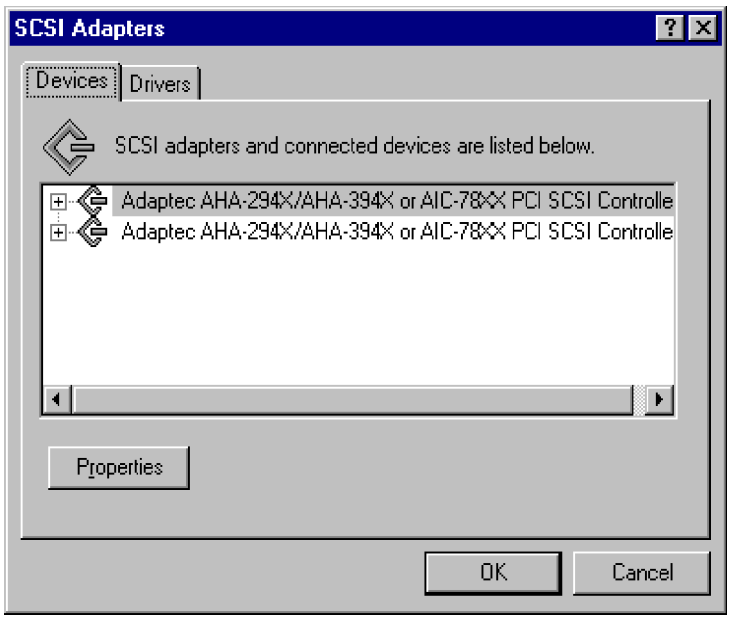
SCSI-sovittimella (SCSI Adapters) asennetaan **SCSI** (*Small Computer Systems Interface*)-ohjainten laiteohjaimia. SCSI on yleinen massamuistien ja oheislaitteiden liitäntämenetelmä tehomikroissa.

Samassa kuvakkeessa tosin hallitaan myös **EIDE** (*Enhanced IDE*)-liitäntäiset ns. ATAPI-standardin mukaiset CD-ROM-asemat, joita Windows NT myös tukee.

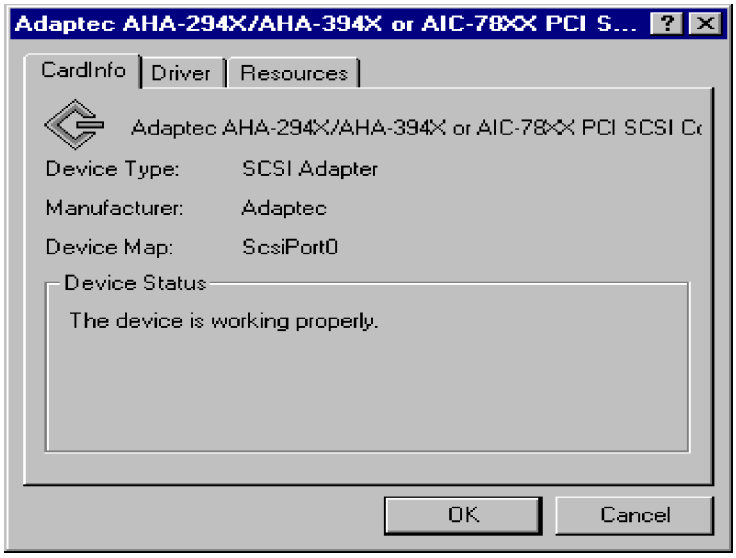
Devices-välilehdestä näet asennetut laitteet (fyysiset ohjaimet) ja **Drivers**-välilehdestä näet asennetut laiteohjaimet eli ajurit asetuksineen.

Devices

Devices-välilehdestä nähdään asennetut SCSI-ohjaimet (sekä IDE-väylän CD-ROM:it, jos niitä on asennettu). Tässä esimerkin palvelimessa on kaksi Adaptecin SCSI-ohjainta: toiseen on liitetty hitaat oheislaitteet, kuten CD-ROM-asemat ja DAT-nauhurit ja toiseen kiintolevyt.



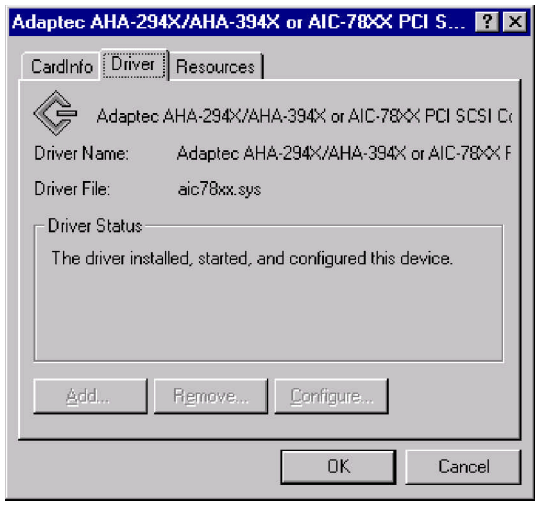
Valitsemalla haluttu ohjain ja painamalla **Properties** saadaan lisätietoja ohjaimesta.



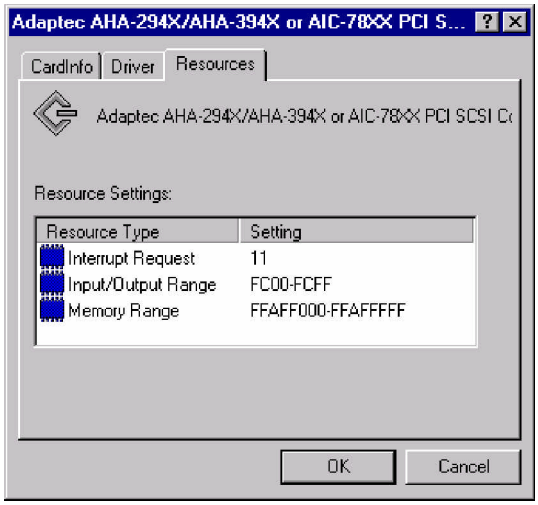
CardInfo-välilehti kertoo seuraavat tiedot:

- **Device type** - laitteen tyyppi (SCSI-ohjain)
- **Manufacturer** - valmistaja
- **Device Map** kertoo rekisterin viittauksen ohjaimelle
- **Device Status** kertoo laitteen toimivan normaalisti.

Driver -välilehti kertoo laiteohjaimen (*Driver*), joka on **aic78xx.sys**:

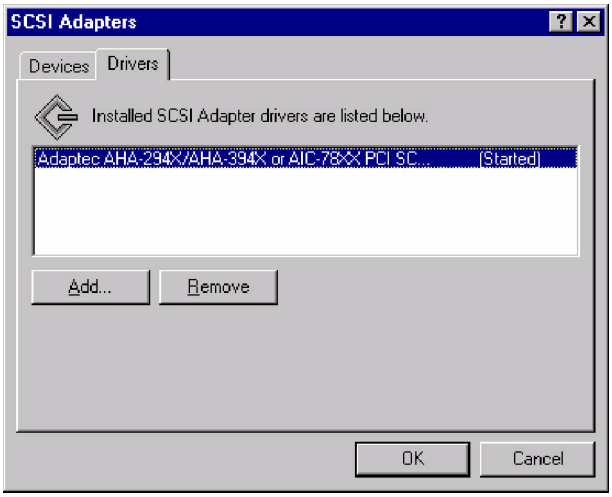


Resources -välilehti kertoo laitteen käyttämät asetukset (keskeytys jne):

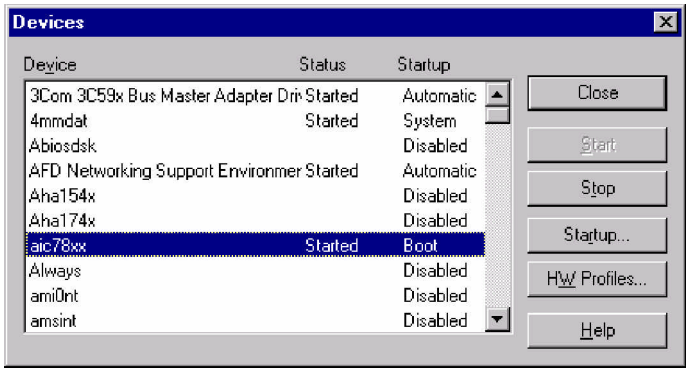


Drivers

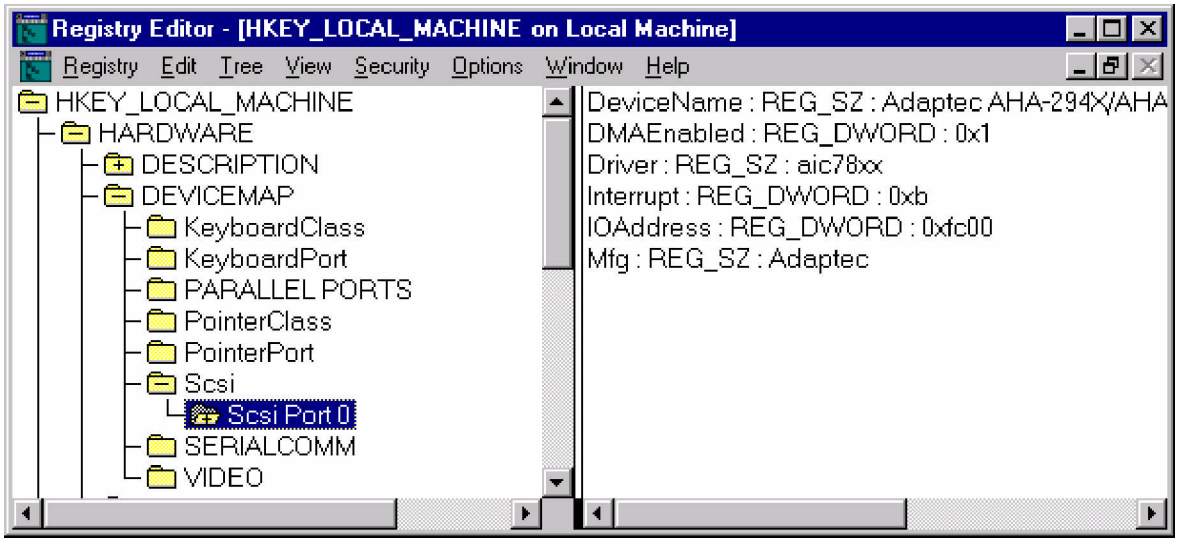
Drivers-välilehdellä voidaan lisätä (**Add**) tai poistaa (**Remove**) asennettuja laiteohjaimia. Samalla nähdään laiteohjaimen tila (**Started**).



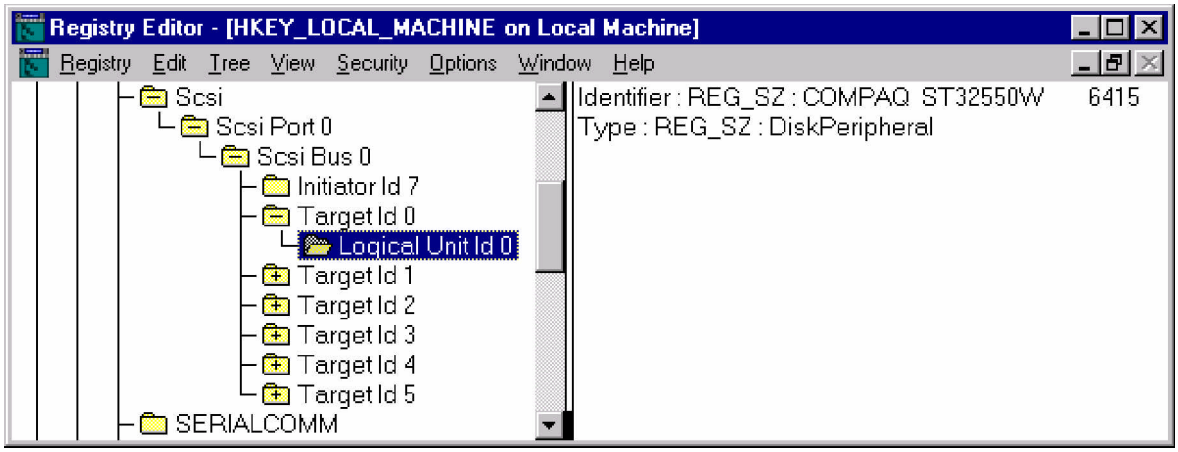
Laiteohjaimen käynnistysasetuksethan löytyvät Ohjauspaneelin **Devices**-kuvakkeen napautuksella. **Aic78xx** on käynnistetty, ja se käynnistetään ensimmäiseksi NT-koneen käynnistyksessä (**Boot**):



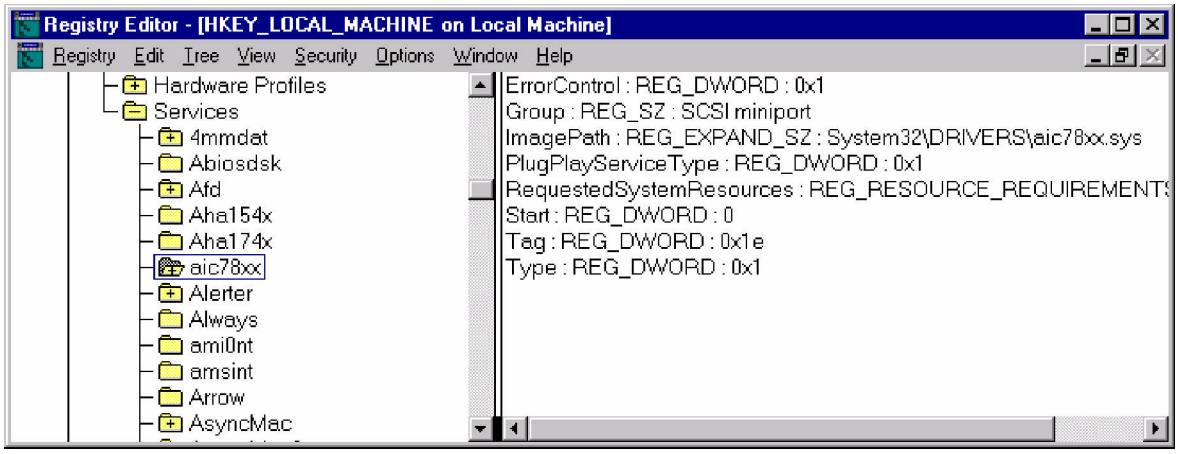
Asetukset tallennetaan rekisteriin ja löytyvät rekisteristä **HKEY_LOCAL_MACHINE\HARDWARE**:n alta. **DEVICEMAP** kertoo laitteiden liitännät - tässä **Scsi**:n alla on **Scsi Port 0**, mikä on esimerkin NT-koneessa ensimmäinen ja ainoa SCSI-ohjain. E.m. asetukset (keskeytys jne) löytyvät näistä asetuksista.



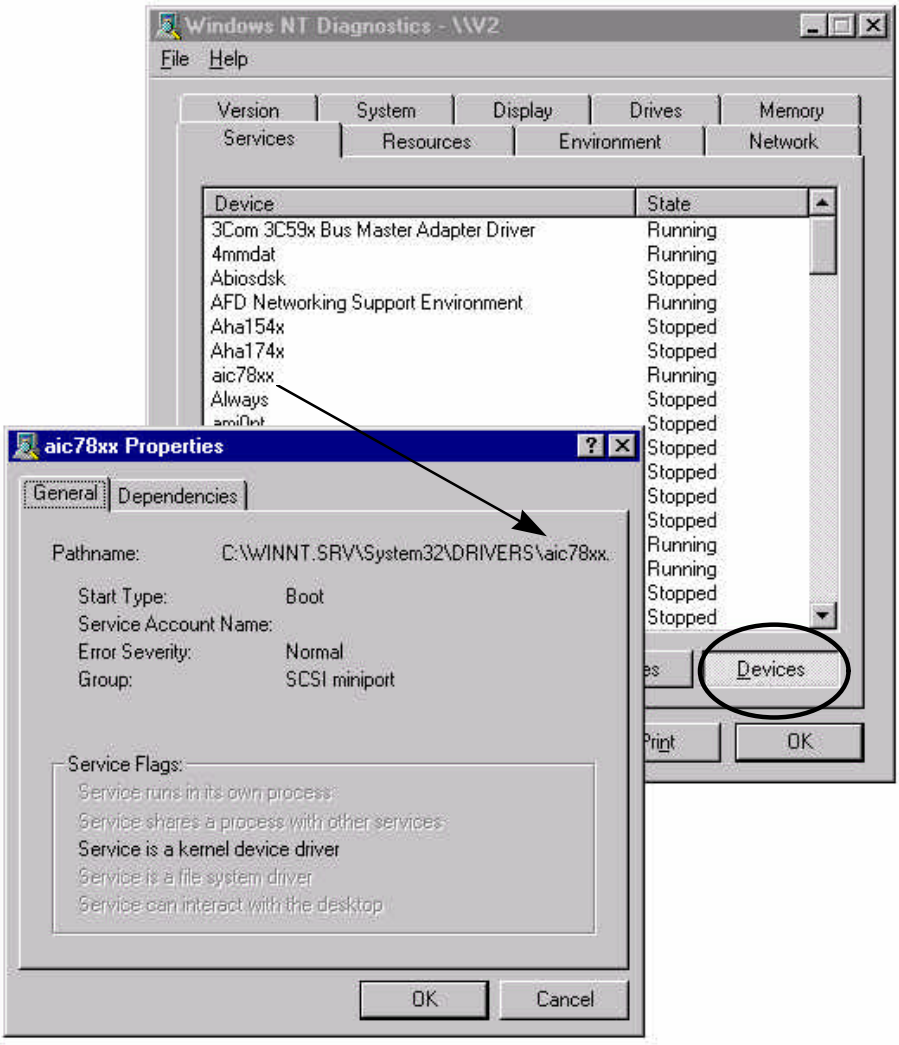
Scsi Port 0:n alla ovat ohjaimeen liitetyt SCSI-oheislaitteet. Koska SCSI-ohjaimessa voi olla useampi väylä, ensimmäinen väylä on **Scsi Bus 0**. Väylän eri laitteet löytyvät a.o. oheislaitteen SCSI-ID:n mukaisesta avaimesta: esimerkin NT-koneessa ensimmäinen (SCSI ID 0) oheislaite on **Compaq St32550w**-kiintolevy.



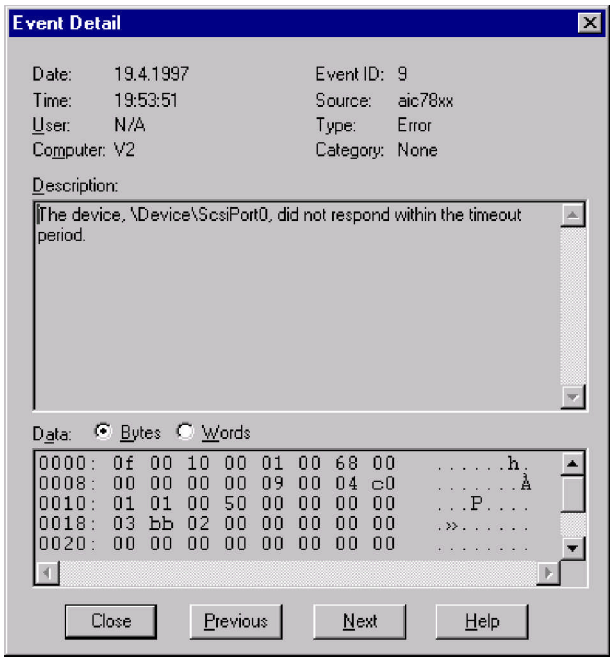
HKEY_LOCAL_MACHINE\SYSTEM:in alta löytyvä **CurrentControlSet\Services** kertoo ohjaimen **aic78xx** (ks. **DEVICEMAP** edellä) fyysisen laiteohjaimen nimen (**aic78xx.sys**).



Tämä löytyy myös **Windows NT Diagnosticsin** avulla; valitse **Services**-välilehti ja **Devices**. Lisätietoja löytyy laiteohjaimen kaksoisnapautuksella tai painamalla **Properties**.



Aic78xx on seurattavissa myös **Event Viewerillä**. Suodatus (**Filter**) voidaan tehdä valitsemalla lähteeksi (**Source**) **aic78xx**. Tässä esimerkissä SCSI-väylään kytketty oheislaite ei ole vastannut aikakatkaisun (*timeout*) puitteissa.



Olipa SCSI-ohjain mikä tahansa, sen antamat virheilmoitukset tulee aina ottaa vakavasti. Jos esimerkiksi edellisenkaltaisia ilmoituksia tulee lokiin muutamia minuutissa, se saattaa olla merkki vakavasta levyongelmasta!

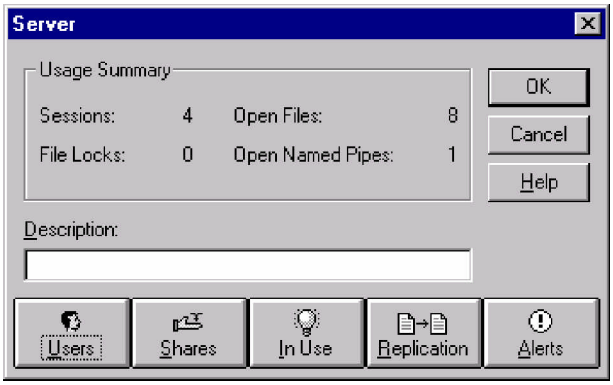
Server

Server-kuvakkeella hallitaan palvelintoimintoja, voidaan muokata NT-koneen mikron kuvausta, saada luettelo NT-koneeseen kirjautuneista käyttäjistä sekä jaetuista ja avoimista resursseista. Tämän lisäksi hallitaan **replikointia** eli **hakemistojen monistamista**. NT-palvelin- ja NT-työasemaversion **Serverin** ero on monistuksessa; vain NT-palvelin voi **viedä** hakemistoja. Sekä NT-palvelin että NT-työasema voi kuitenkin **tuoda** hakemistoja. Lisäksi voidaan käsitellä luetteloa järjestelmän hälytysten vastaanottajista. **Serverin** toiminnot voidaan hoitaa toiselta NT-koneella **Server Managerilla** valitsemalla haluttu kohteeksi haluttu NT-kone.

Kaksoisnapautettuasi kuvaketta näet heti yhteenvedon palvelimen tilanteesta. Voit muuttaa palvelimen kuvausta kirjoittamalla **Description**-ruutuun uuden kuvauksen.

Alareunassa on viisi painiketta:

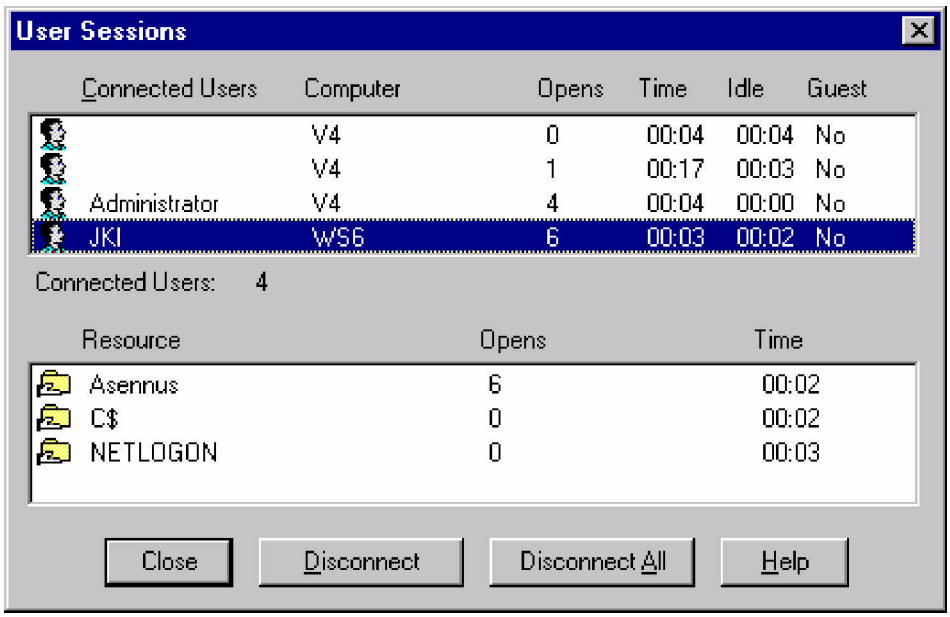
- **Users** - palvelimeen liittyneiden käyttäjien selailu
- **Shares** - jaettujen resurssien käytön selailu
- **In Use** - käytössä olevien resurssien selailu
- **Replication** - hakemistojen/tiedostojen kopiointipalvelu
- **Alerts** - hälytysten asettaminen.



Users

Tällä painikkeella nähdään palvelimeen liittyneet käyttäjät.

User Sessions-valintaikkunan **Connected Users** -listassa on luettelo tällä hetkellä palvelimeen/työasemaan etäyhteydessä olevista käyttäjistä. Näet **Resource**-listassa yhden käyttäjän avaamat resurssit valitsemalla ensin listasta käyttäjätunnuksen.



Voit katkaista halutun käyttäjän palvelinyhteyden valitsemalla ensin käyttäjänimi **Connected Users** -listasta ja painamalla sitten **Disconnect**-painiketta.

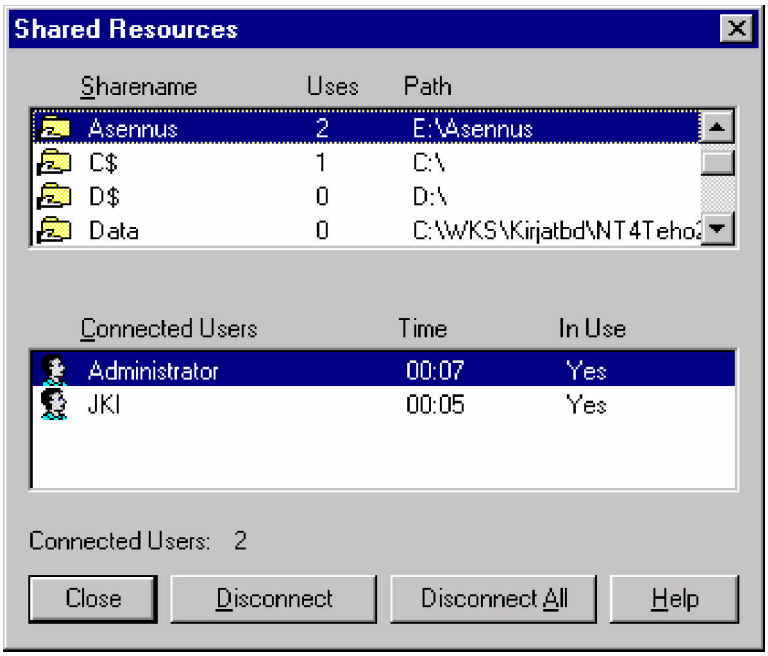
Voit tarvittaessa katkaista kaikkien käyttäjien kaikki palvelinyhteydet painamalla **Disconnect All**-painiketta.

Muista ensin ilmoittaa käyttäjille vaikkapa **Server Managerin Send Message**-toiminnon tai komentorivin **NET SEND**-komennolla, että palvelinyhteydet katkaistaan!

Shares

Jaettujen resurssien käytön selailu onnistuu **Shares**-painikkeella. Voit katkaista halutun käyttäjän palvelinyhteyden valitsemalla ensin jaetun resurssin nimi **Sharename** -listasta ja valitsemalla halutun käyttäjän **Connected Users** -listasta ja painamalla sitten **Disconnect**-painiketta.

Voit tarvittaessa katkaista kaikkien käyttäjien kaikki palvelinyhteydet jaettuun resurssiin painamalla **Disconnect All** -painiketta.

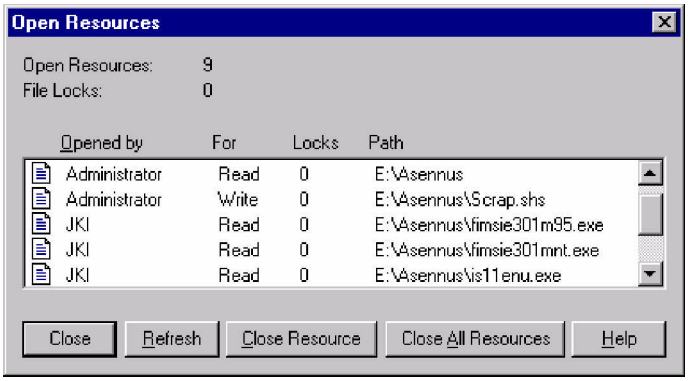


Windows NT-palvelimessa on tyypillisesti seuraavia oletusjakoja:

Jakonimi	Hakemisto	Tarkoitus
ADMIN$	%Systemroot%	Järjestelmän etähallinta
C$	C:\	Levyaseman juurihakemisto - saa käyttöön vain pääkäyttäjän (Administrator)-tason oikeuksin
IPC$	Nimetty putki (Remote IPC)	Järjestelmän etähallinta
NETLOGON	%Systemroot%\System32\Repl\Import\Scripts	Kirjauskomentojonot, Default User-hakemisto, NTConfig.pol
PRINT$	%Systemroot%\System32\Spool\Drivers	Kirjoitinohjaimet

In Use

Käyttäjien palvelimelta/työasemasta käytössä olevien resurssien selailu; **Open Resources**-valintaikkunassa **Opened By**-listassa on käyttäjän nimi, joka avasi resurssin.



Sulje yksittäinen resurssi valitsemalla ensin resurssi luettelosta ja sitten **Close Resource** -painike. Sulje kaikki resurssit valitsemalla **Close All Resources** -painike.

Päivitä valintaikkunan tiedot valitsemalla **Refresh**-painike.

Replication

Kansioiden/tiedostojen kopiointipalvelu: **Export**-vientimonistuksen voi suorittaa vain Windows NT -palvelin, ei Windows NT -työasema. **Import**-tuontimonistuksen voi sen sijaan suorittaa myös Windows NT -työasema.

Varmista, että **Directory Replicator** -palvelulle on määritetty sopiva käyttäjätunnus:

- Käyttäjätunnuksen on kuuluttava **Replicator**-ryhmään
- Käyttäjätunnuksella on oltava oikeus (**User Right**) kirjautua palveluna (**Log on as a service**). Tämän voit asettaa **User Manager for Domainsilla** valitsemalla **Policies** | **User Rights** avulla.

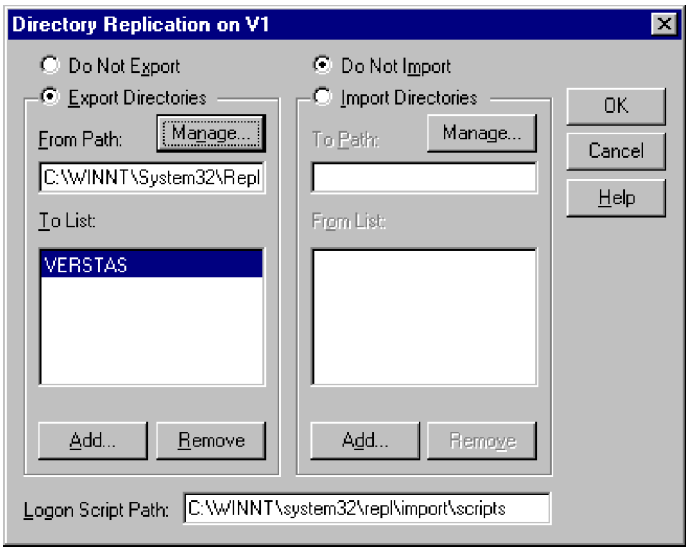
Vientipalvelimen määrittäminen:

1) Luo ensin ne hakemistot **Winnt\System32\Repl\Export**-hakemistoon, jotka haluat viedä. Lisää halutessasi vietävät tiedostot alihakemistoihin; lisääminen ei ole tässä vaiheessa pakollista. Kun monistus on käynnistynyt, alihakemistoihin myöhemmin lisätyt tiedostot viedään automaattisesti

2) Valitse Ohjauspaneelin **Server**-ohjelman **Replication** -painike ja valitse **Export Directories**

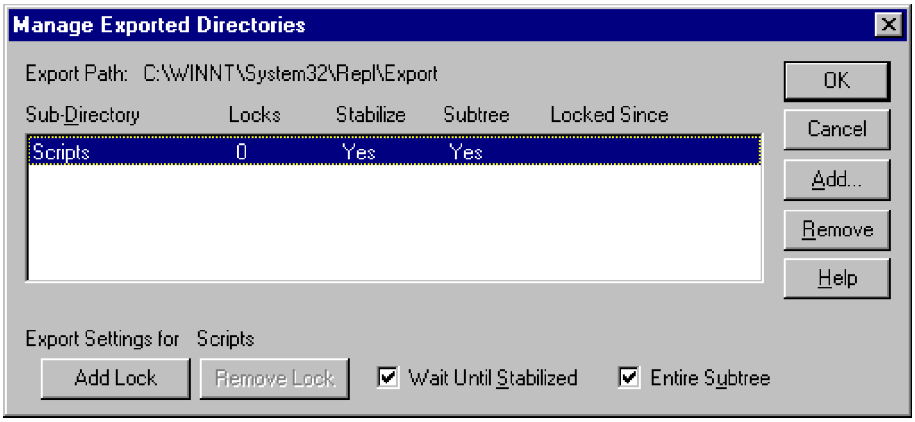
3) Vaihda tarvittaessa vietävien alihakemistojen päähakemisto kirjoittamalla **From Path**-ruutuun toinen polku

4) Vie alihakemistot haluttuun toimialueeseen (myös niihin, joihin on luottosuhde) tai yksittäiseen palvelimeen/työasemaan valitsemalla **To List**-ryhmän **Add**-painike ja valitsemalla tai kirjoittamalla tarvittavat tiedot **Select Domain**-valintaikkunaan. Tämän jälkeen valitsemasi toimialueen tai palvelimen/työaseman nimi tulee **To List**-ruutuun



Oletuksena **To List**-ruutu on tyhjä ja vienti tapahtuu automaattisesti paikalliselle toimialueelle; jos ruutuun lisätään jokin työasema/palvelin, vienti ei enää jatku paikalliselle toimialueelle; tällöin toimialueen nimi on tarvittaessa lisättävä erikseen **To List**-ruutuun.

5) Määritä lukitusten (*locks*), vakauttamisen (*stabilization*) ja alihakemistojen (*subtree*) monistamiseen liittyvät asetukset alihakemistoille valitsemalla **Manage** -painike.



Asetukset ovat seuraavat:

- **Sub-Directory** - kertoo vietävän hakemistopolun
- **Locks** - lukituksella estetään haluttaessa kyseisen hakemiston vienti. Voit käyttää painikkeita **Add Lock** ja **Remove Lock**

- **Stabilize** - **Yes** vie hakemiston vasta kahden minuutin kuluttua tiedostojen muutoksista; oletusarvo **No** vie tiedostot heti. Voit muuttaa arvoa napauttamalla **Wait Until Stabilized**-painiketta

- **Subtree** -alihakemistot; **Yes** on oletusarvo ja vie myös valitun hakemiston alihakemistot; **No** ei vie

- **Locked Since** - kertoo milloin lukitus lisättiin

- **Export Settings for**-asetukset:

  - **Add Lock** - lisää lukituksen
  - **Remove Lock** - poistaa lukituksen
  - **Wait Until Stabilized**- voit muuttaa vakautuksen tilaa
  - **Entire Subtree** - viedäänkö koko hakemistorakenne alihakemistoineen.

  Määritä tarvittaessa lisäasetukset. Paina **OK**

6) Lopeta valitsemalla **Directory Replication**-valintaikkunasta **OK**.

Huomattavaa:

- Jos vientimonistuksessa tarvittavaa **REPL$**-jakonimeä ei ole määritetty, järjestelmä luo sen. Jaettava hakemisto on NT-systeemihakemiston alihakemisto, esimerkiksi **C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS**.

- Jos **Directory Replication** ei ole jo käynnissä, järjestelmä käynnistää sen.

- Lopeta alihakemistojen vienti toimialueelle tai tietokoneeseen valitsemalla ensin haluttu toimialue tai palvelin/työasema ja valitsemalla **Remove**-painike

Tuontimonistuksen määrittäminen **Windows NT -työasemassa tai -palvelimessa** (siksi esimerkissä myös suomenkielinen Windows NT 4.0-työasema):

1) Varmista ensin **Käyttäjien hallinnalla** (User Manager), että työaseman/palvelimen **Hakemiston monistus** (Directory Replicator)-palvelulle on määritetty sopiva käyttäjätunnus. Käyttäjätunnuksen on kuuluttava paikalliseen **Monistus** (Replicator)-ryhmään; vähimmällä pääset kun lisäät sen kyseisestä toimialueesta

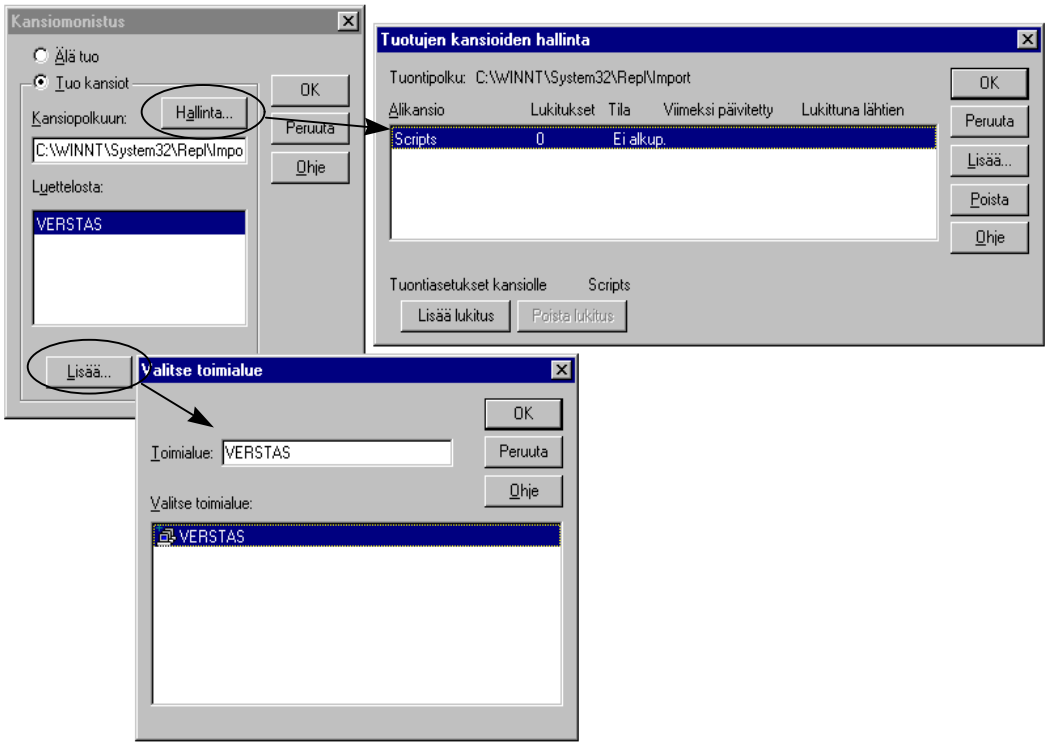
2) Määrittele palvelun käynnistys: Valitse **Ohjauspaneelin** (Control Panel) **Palvelut** (Services)-ohjelma ja valitse **Hakemistojen monistus** (Directory Replication). Määrittele **Käynnistystyypiksi** (Startup Type) **Automaattinen** (Automatic) ja valitse **Kirjautumisnimeksi** (Log On As) edellä määritelty käyttäjätunnus. Kirjoita salasanat ja paina **OK**

Tämän jälkeen palvelun tulisi käynnistyä ja siitä kertova ikkuna tulee näyttöön.

3) Valitse **Ohjauspaneelin** (Control Panel) **Palvelin** (Server)-ohjelman **Monistus** (Replication) -painike ja valitse **Tuo hakemistot** (Import Directories)

4) Tuo hakemistot halutusta toimialueesta (myös niihin, joihin on luottosuhde) tai yksittäisestä palvelimesta valitsemalla **Luettelosta** (From List)-ryhmän **Lisää** (Add)-painike ja valitsemalla tai kirjoittamalla tarvittavat tiedot **Valitse toimialue** (Select Domain)-valintaikkunaan. Tämän jälkeen valitsemasi toimialueen tai palvelimen nimi tulee **Luetteloon** (To List)-ruutuun

5) Määritä lukitusten (*locks*), vakauttamisen (*stabilization*) ja alihakemistojen (*subtree*) monistamiseen liittyvät asetukset alihakemistoille valitsemalla **Hallinta** (Manage) -painike



Asetukset ovat seuraavat:

- **Tuontipolku** (Import Path) - hakemistopolku, jonne tuodaan
- **Alihakemisto** (Sub-Directory) - tuotava alihakemisto
- **Lukitukset** (Locks) - lukituksella estetään haluttaessa kyseisen hakemiston tuonti. Voit käyttää painikkeita **Lisää lukitus** (Add Lock) ja **Poista lukitus** (Remove Lock). Hakemistoon voi lisätä useammankin lukituksen; tuonti tulee vain jos arvo on **0**
- **Tila** (Status) - **OK** tilanne on normaali; **Ei alkuperäistä** (No Master) vientipalvelu ei mahdollisesti toimi palvelimessa; **Ei tahdistusta** (No Sync) tiedostoja on joskus monistettu, mutta nyt ne eivät ole ajantasalla; jos **ei ole mitään merkintää**, tietoja ei ole koskaan tuotu
- **Viimeisin päivitys** (Last Update) - milloin tietoja on viimeksi tuotu

- **Lukittuna lähtien** (Locked Since) - milloin lukitus lisättiin

Tuontiasetukset hakemistolle (Import Settings for)-asetukset:

- **Lisää lukitus** (Add Lock) - lisää lukituksen
- **Poista lukitus** (Remove Lock) - poistaa lukituksen.

Määritä tarvittaessa lisäasetukset. Paina **OK**

6) Lopeta valitsemalla **Hakemistomonistus** (Directory Replication)-valintaikkunasta **OK**.

Kirjauskomentojonojen monistusta on käsitelty **luvussa 5**.

Alerts

Hälytysten asettaminen tehdään **Alerts**-painikkeella. Voit määrittää käyttäjät ja työasemat tai palvelimet (NetBIOS-nimet), jotka saavat ilmoituksen tässä mikrossa tapahtuvista **hallinnollisista eli valvontahälytyksistä**. Ne tulevat järjestelmästä ja liittyvät palvelimen/resurssien käyttöön varoittaen suojaus- ja käyttöoikeusongelmista, istuntoihin liittyvistä ongelmista, kirjoitinongelmista sekä palvelimen sammuttamisesta virtakatkoksen vuoksi, kun UPS-palvelu on käytössä.

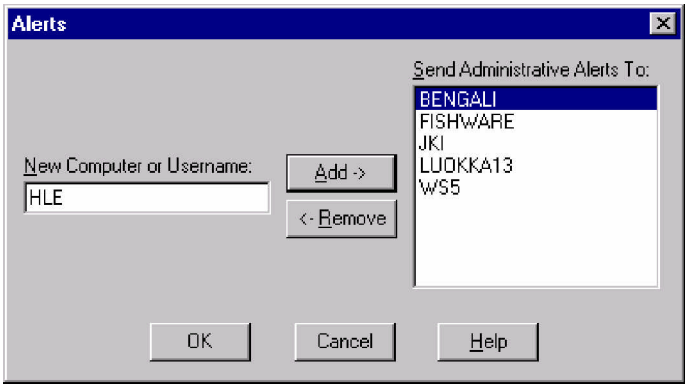
Hallinnollisten hälytysten vastaanottajien valinta tehdään seuraavasti:

1) Valitse **Server**-valintaikkunasta **Alerts**

2) Lisää käyttäjä tai mikro hälytysten vastaanottajaluetteloon kirjoittamalla ensin **New Computer or Username**-ruutuun haluamasi nimi ja valitsemalla sitten **Add**-painike

3) Paina lopuksi **OK**

Poista käyttäjä tai tietokone hälytysten vastaanottajaluettelosta valitsemalla **Send Administrative Alerts**-ruudusta haluamasi nimi ja sitten painamalla **Remove**-painiketta.

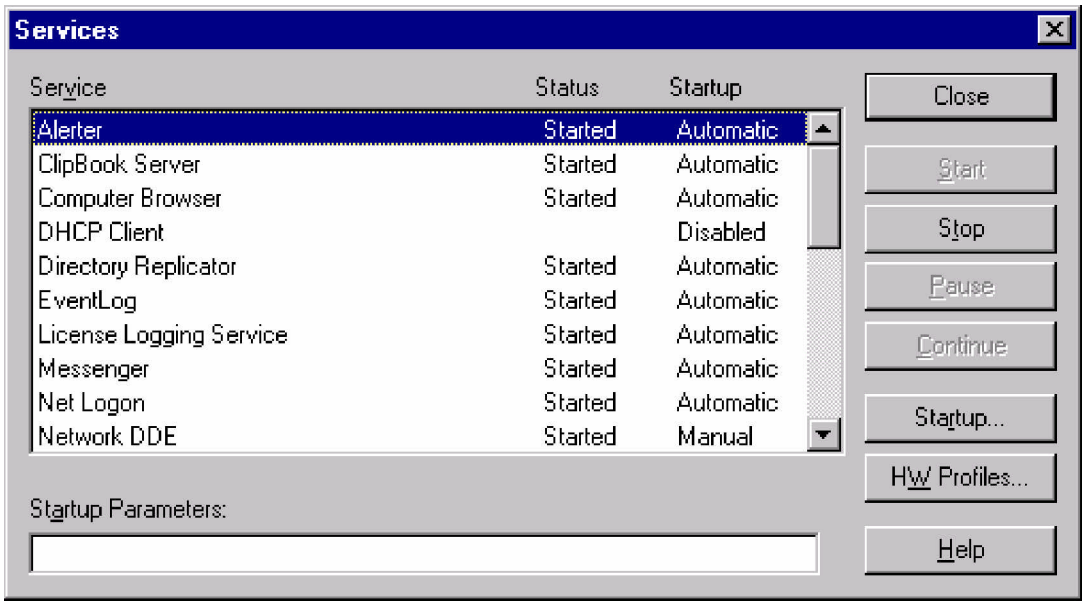


Esimerkissä **BENGALI** ja **FISHWARE** ovat toimialueiden nimiä, **JKI** ja **HLE** käyttäjätunnuksia, **WS5** työaseman nimi ja **LUOKKA13** on **työryhmän** nimi.

Services

Services on järjestelmän palveluiden hallinta. Voit lopettaa, aloittaa, keskeyttää tai jatkaa palvelimessa käytettävissä olevia palveluja, lähettää niille käynnistysparametreja ja määrittää palvelujen käynnistysasetukset.

Palvelut ovat etähallittavissa **Server Managerin** avulla.



Windows NT-palvelimen mukana tulevat palvelut ovat konfiguraatiosta riippuen seuraavat:

- **Alerter** - hälytyspalvelu
- **ClipBook Server** - leikekirjapalvelin (on erikseen käynnistettävä palvelimessa) - **Edit** | **Copy** / **Edit** | **Paste**- ja leikekirjan tarkastelu **Clipbook Viewer** käyttää tätä palvelua
- **Computer Browser** on selauspalvelu - ainakin palvelimissa syytä olla käytössä, jotta selauspalvelu toimii ja työasemissa voi selata verkkoa
- **DHCP Client** - palvelin saa DHCP:n avulla IP-osoitteen ja -asetukset
- **Directory Replicator** on hakemiston monistuspalvelu, erikseen käynnistettävä, kuitenkin vain jos NT-kone osallistuu monistukseen
- **EventLog** on tapahtumaloki - käynnistyy automaattisesti, tallentaa tapahtumalokia
- **FTP Publishing Service** - Internet Information Server-palvelimen FTP-palvelin, jos asennettu

- **Gopher Publishing Service** - Internet Information Server-palvelimen Gopher-palvelin, jos asennettu
- **License Logging Service** - lisenssien hallintapalvelu
- **Messenger** on viestinvälityspalvelu. Tämän avulla NT-kone voi lähettää sanomia
- **Microsoft DHCP Server** - DHCP-palvelin, jos asennettu
- **Microsoft DNS Server** - DNS-palvelin, jos asennettu
- **Net Logon** - kirjautumispalvelu; palvelimissa **syytä** olla käytössä, jotta käyttäjien verkkoonkirjautuminen toimii! Myös NT-työasemien toimialueelle kirjautuminen hoidetaan NT-työaseman Net Logon-palvelun avulla
- **Network DDE**, verkko-DDE (*Dynamic Data Exchange*), erikseen käynnistettävä)
- **Network DDE DSDM** (NetDDE DSSM (*DDE share database manager*), erikseen käynnistettävä
- **Network Monitor Agent** - verkkomonitorin agentti, erikseen asennettava ja käynnistettävä
- **NT LM Security Support Provider** - NT LM suojausjärjestelmä, käynnistetään automaattisesti tarvittaessa
- **OLE** - OLE-palvelu (*Object Linking and Embedding*), erikseen käynnistettävä
- **Plug and Play** - Kytke-ja-käytä-tuki, käynnistetään automaattisesti tarvittaessa
- **Remote Access Autodial Manager** - puhelinyhteyksien automaattinen avaus, käynnistetään automaattisesti tarvittaessa
- **Remote Access Connection Manager** - puhelinyhteyspalvelu, käynnistetään automaattisesti tarvittaessa
- **Remote Access Server** - etäkäyttöpalvelin, käynnistetään automaattisesti

- **Remote Procedure Call (RPC) Locator** - etäproseduurikutsujen (RPC) paikannin
- **Remote Procedure Call (RPC) Service** - etäproseduurikutsujen (RPC) palvelu
- **RIP for Internet Protocol** - RIP-palvelu IP-protokollalle
- **Schedule** - ajoituspalvelu, erikseen käynnistettävä - jos esimerkiksi halutaan käyttää AT-komentoa
- **Server** - ainakin palvelimissa syytä olla käytössä, jotta palvelinpalvelu toimii
- **Simple TCP/IP Services** - jos asennettu, niin echo, discard jne käytettävissä
- **SNMP** - SNMP-palvelu
- **SNMP Trap Service** - SNMP-hälytykset
- **Spooler** - tulostuspalvelu - sekä tulostuspalvelin että sovellukset tulostavat tämän avulla
- **TCP/IP NetBIOS Helper** - jos TCP/IP on käytössä
- **Telephony Service** - puhelinyhteyspalvelu (jos asennettu)
- **UPS** - jos UPS on kytketty
- **Windows Internet Name Service** - WINS-palvelin (jos asennettu)
- **Workstation** - työasemapalvelu, syytä olla käytöss myös palvelimissa, jotta muuta palvelut toimivat
- **World Wide Web Publishing Service** - Internet Information Server-palvelimen WWW-palvelin (jos asennettu).

Services-valintaikkunasta käynnistetään, pysäytetään tai keskeytetään käytettävissä olevia palveluja ja jatketaan niitä sekä määritetään palvelujen valinnaiset käynnistysparametrit.

Server-palvelinpalvelun pysäyttäminen katkaisee kaikkien verkkokäyttäjien yhteyden tietokoneeseen. Varoita käyttäjiä, ennen kuin pysäytät palvelun.

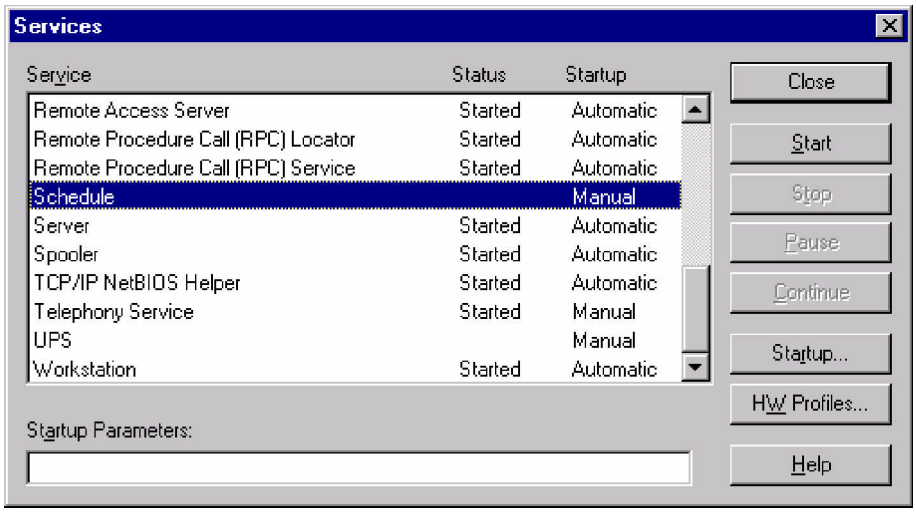
Palvelujen käynnistäminen, pysäyttäminen, keskeyttäminen tai jatkaminen tehdään seuraavasti:

1) Valitse **Services**-valintaikkunasta haluamasi palvelu

2) Valitse käynnistä **Start**, pysäytä **Stop**, keskeytä **Pause** tai jatka **Continue**-painikkeella. Jos haluat määrittää valinnaiset käynnistysparametrit palvelulle, kirjoita ne **Startup Parameters**-ruutuun, ennen kuin valitset **Startup**-painikkeen

3) Valitse lopuksi **Close**-painike.

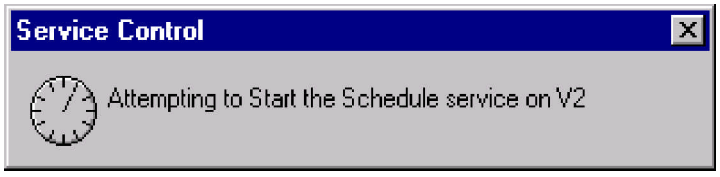
Esimerkiksi käytettäessä ajastettuja toimintoja (kuten komentorivin **AT**-komentoa) tarvitaan **Schedule**-palvelu.



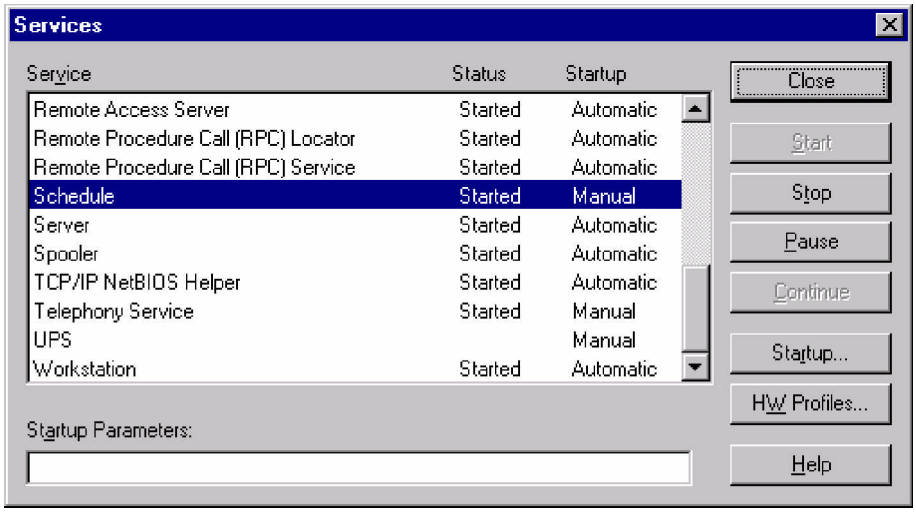
Se käynnistetään seuraavasti:

1) Valitse **Services**-valintaikkunasta **Schedule**-palvelu

2) Valitse **Start**. Näyttöön tulee ilmoitus, että palvelu käynnistetään

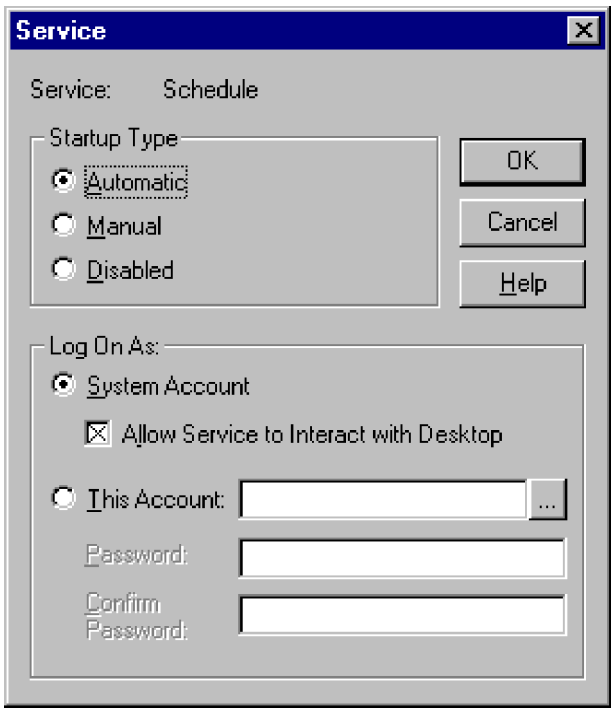


3) Nähdään, että palvelu käynnistyi.



Valitse lopuksi **Close**-painike.

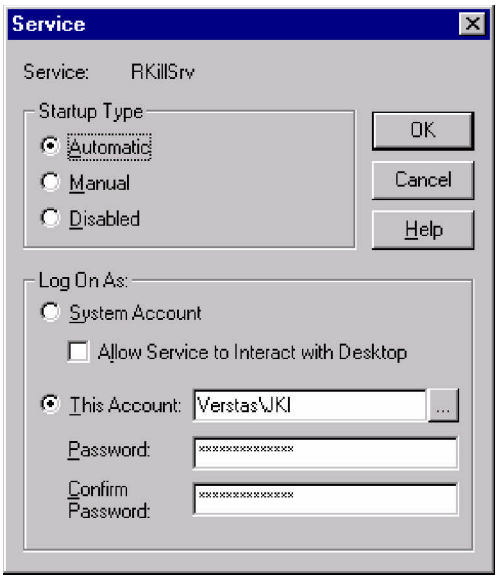
Tällä menetelmällä palvelu käynnistyy vain NT:n käytön ajaksi. Voit määritellä palvelun käynnistymään aina automaattisesti. Valitse tällöin **Startup...**-painike ja valitse **Automatic**.



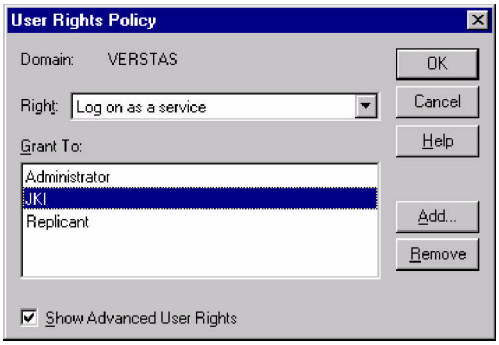
Muita valintoja ovat **Manual**, jolloin palvelu on aina erikseen käynnistettävä ja **Disabled**, jolloin palvelu ei ole käytettävissä.

Jotkin palvelut edellyttävät kirjoittautumista järjestelmään **tietyllä käyttäjätunnuksella** (Log On As). Tällaisia palveluita saattavat olla eräät tietokantapalvelintoiminnot, sanomanvälityspalvelut ja esimerkiksi edellä käsitelty hakemistojen monistuspalvelu. Anna tällöin a.o. käyttäjätunnus ja salasana niille varattuun kohtaan. Voit määrittää palvelun käynnistysasetukset vain, jos olet kirjautunut pääkäyttäjien Administrators-ryhmän käyttäjänä.

Valitse **Allow Service to Interact with Desktop**, jos palvelu tarvitsee käyttäjän toimenpiteitä (näppäimen painallus tms).



Anna kyseiselle käyttäjätunnukselle myös oikeus kirjautua palveluna **User Manager for Domains**in **Policies** | **User Rights** -valinnalla. Valitse Show Advanced User Rights, niin voit lisätä käyttäjätunnuksen oikeuteen **Log on as a service**.



Käynnistetyt palvelut näet myös komentorivin **NET START** -komennolla. vastaavasti voit käynnistää palvelun **NET START** -komennolla, esimerkiksi **NET START SCHEDULE**. Palvelun voit pysäyttää komennolla **NET STOP palvelunnimi**, esimerkiksi **NET STOP SCHEDULE**. Etähallinta onnistuu **Server Manager**illa tai **NETSVC**:llä.

System

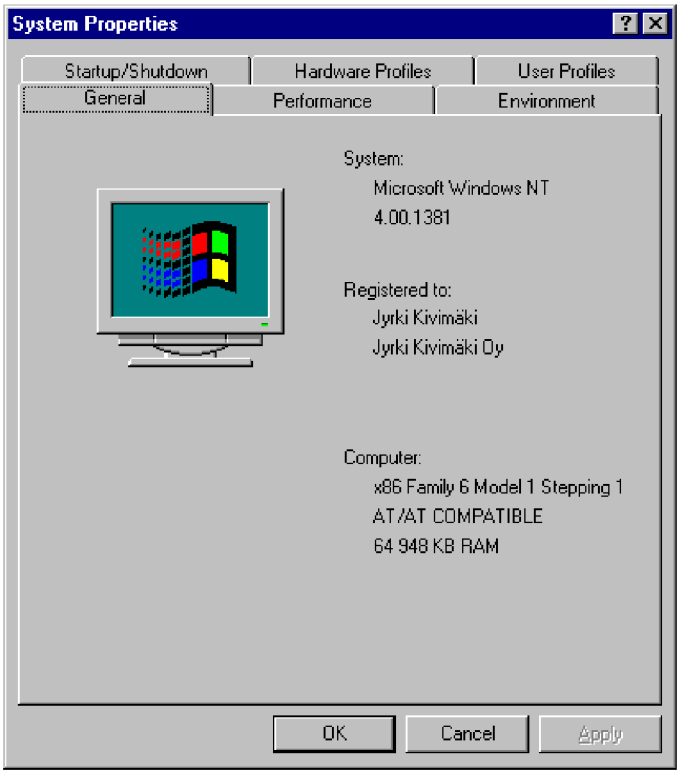
System-kuvakkeen avulla hallitaan laitteiston ja käyttöjärjestelmän asetukset, mm. sivutustiedoston ja käyttöjärjestelmän käynnistyksen asetukset.

Välilehdet ovat seuraavat:

- **General** - yleiset tiedot
- **Performance** -sivutustiedoston asetus
- **Environment** - ympäristömuuttujat
- **Startup/Shutdown** - käynnistys/sammutusasetukset
- **Hardware Profiles** - laitteistoprofiilit
- **User Profiles** - käyttäjäprofiilien hallinta.

General

General -välilehti kertoo lyhyesti ja ytimekkäästi Windows NT:n tarkan versionumeron, kenelle se on **rekisteröity** (Registered), suorittimen tyypin sekä keskusmuistin (fyysisen RAM-muistin) määrän.

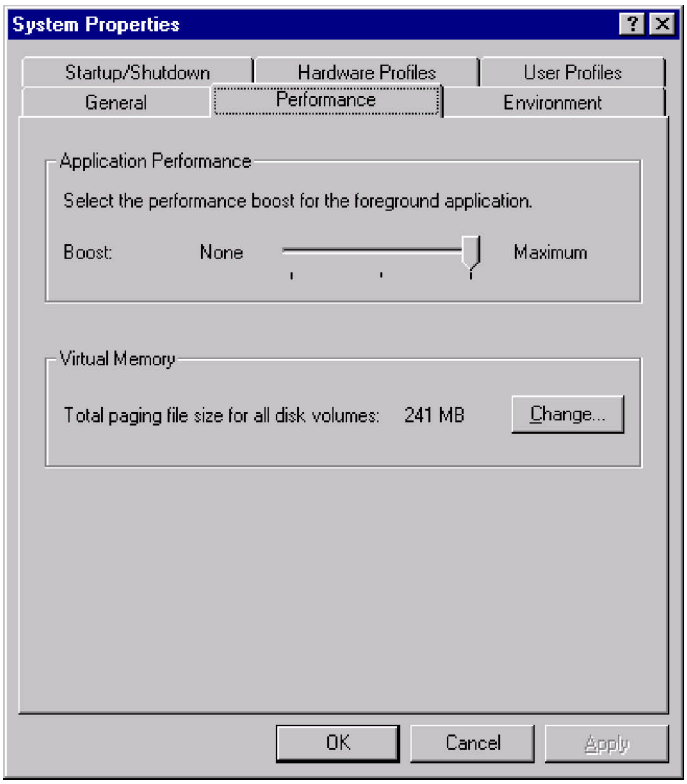


Rekisteröintiasetukset löytyvät rekisteristä polusta

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion.

Performance

Application Performance-asetuksen avulla määritellään paikallisen työaseman moniajon asetukset: saako edustalla ajettava sovellus eniten aikaa (osoitin on oikeassa reunassa **Maximum**) vaiko molemmat yhtä paljon (lisäys on **None**).

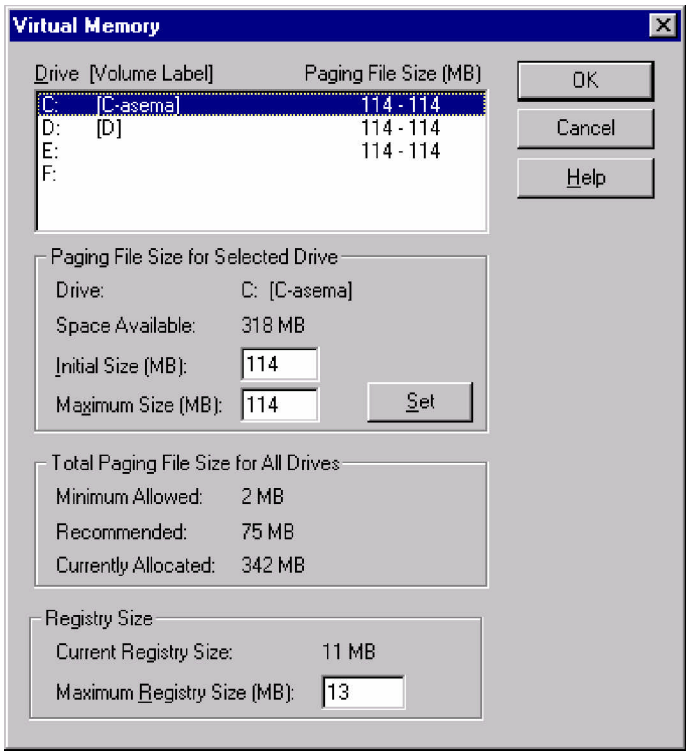


Palvelimella kannattaa olla varovainen **Boost**-asetuksen kanssa; jos ajat jotakin monitoria palvelimen näytössä (ja sovellus odottaa koko ajan käyttäjän näppäimenpainallusta, esimerkiksi **Press Ctrl+C**), niin CPU-kuormitus saattaa nousta yllättäen 100 prosenttiin!

Virtual Memory -näennäismuistin **Change**-painikkeen avulla saadaan näyttöön **Virtual Memory** -ikkuna, jonka avulla määritellään näennäismuistin asetukset.

Sivutustiedoston (**Paging File**) sijainti, alkuperäinen koko ja suurin mahdollinen koko voidaan asettaa tämän kautta. Nämä asetukset määritellään jo NT:n asennusvaiheessa; suosituksena on **fyysinen keskusmuisti + 12 MT**. Jos keskusmuistia siis on 64 Mt, niin jatkettua muistia on 63 Mt. Sivutustiedosto on tällöin **63 Mt + 12 Mt = 75 Mt**.

Esimerkin palvelimessa on käsin laajennettu sivutustiedostoa useammalle fyysiselle levylle sekä sivutustiedoston kokoa on kasvatettu. Se on kiinteän mittainen kaikilla kolmella levyasemalla (jotka ovat kukin fyysisiä levyasemia):



Sivutustiedoston muuttaminen tehdään seuraavasti (sinun on oltava paikallisen Administrators-ryhmän jäsen):

1) Valitse **Drive**-ruudusta asema, jonka sivutustiedoston koon haluat muuttaa

2) Kirjoita **Paging File Size for Selected Drive**-ryhmän ruutuihin sivutustiedoston uusi **Initial Size**-aloituskoko- tai **Maximum Size**-enimmäiskoko megatavuina. Valitse lopuksi **Set**-painike ja palaa takaisin valitsemalla **OK**.

Sivutustiedoston määrittelyyn pätee muutama sääntö:

- Sivutustiedoston koko ei missään tilanteessa saa olla pienempi kuin fyysisen keskusmuistin määrä, varsinkaan järjestelmälevyllä (levyasema, jonne Windows NT on asennettu). Se hankaloittaa NT:n elpymistä ongelmatilanteissa

- Windows NT:n käytön aikana sivutustiedostoa **PAGEFILE.SYS**-tiedostoa et voi poistaa; jos poistat tiedoston käynnistettyäsi mikron MS-DOS:iin, seuraavassa NT:n käynnistyksessä luodaan uusi. Rekisterin asetuksella voit kuitenkin poistaa sivutustiedoston, kun järjestelmä suljetaan

- Riippuen järjestelmäsi kokoonpanosta tehokkaimmin näennäismuisti toimii, jos jaat sivutustiedoston useammalle fyysiselle kiintolevylle. Kuitenkin RAID-levyjärjestelmällä varustetuissa palvelimissa jo laitteisto huolehtii kuormituksen jakamisesta eri levyille

- Koska sivutustiedosto kasvaa tarvittaessa dynaamisesti, sivutustiedoston levyllä tulisi **aina** olla riittävästi vapaata levytilaa. Tämä on erityisen tärkeää palvelimissa.

Rekisterin maksimikoko asetetetaan **Maximum Registry Size** -asetuksella. Näet samalla, paljonko rekisteri tällä hetkellä vaatii muistia.

Muuta asetusta vain erityisistä syistä, kyse on tavallisesti toimialueen ohjauskone (*domain controller*)-tyyppisistä palvelimista.

Environment

Ympäristömuuttujat (*Environment Variables*) ovat asetuksia, joita sovellukset voivat lukea, tarvittaessa muuttaa ja poistaa. Windows NT:n käynnistyksessä ympäristömuuttujat alustetaan ja niille varataan muistista tilaa, johon ympäristömuuttujat talletetaan. Ympäristömuuttujalla on jokin nimi sekä sille on asetettu jokin arvo. Arvoa voidaan tarvittaessa muuttaa sekä ympäristömuuttuja voidaan ottaa pois käytöstä. Ympäristömuuttujat voidaan asettaa kahdella eri tavalla: **Environment**-välilehdessä sekä **komentorivillä SET**-komennolla. Ympäristömuuttujat saat myös esille komentorivillä komennolla **SET**.

Kaikki käyttäjät voivat asettaa käyttäjäkohtaisia ympäristömuuttujia, mutta Administrators-ryhmän jäsenet voivat asettaa myös koko järjestelmää ja kaikkia käyttäjiä koskevia järjestelmämuuttujia (*System Variables*). Kaikki nämä asetukset tallennetaan rekisteritietokantaan, josta ne luetaan kirjauduttaessa järjestelmään.

Järjestelmämuuttujat (*System Variables*) ovat seuraavat:

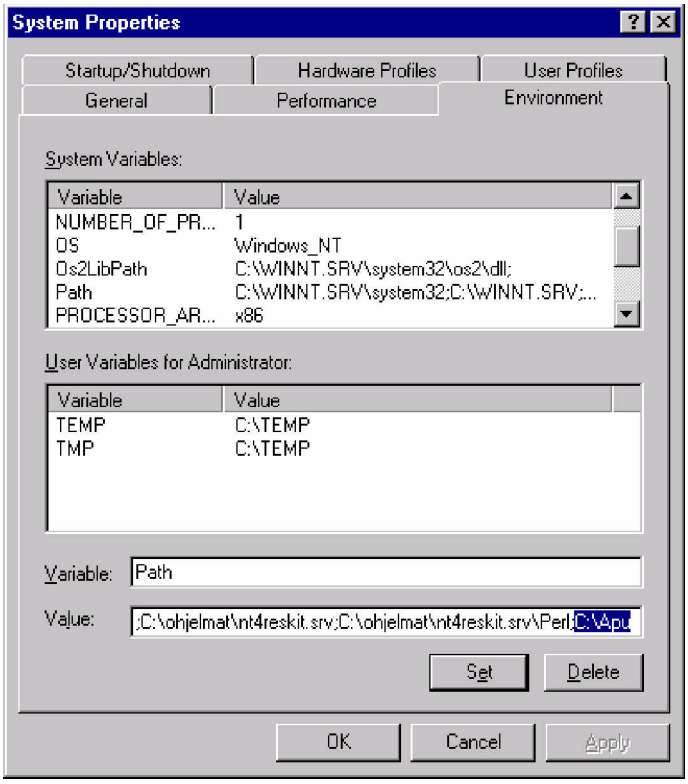
Ympäristömuuttuja	Merkitys
ComSpec	Komentotulkin sijainti
NUMBER_OF_PROCESSORS	Tietokoneen prosessorien lukumäärä
OS	Käyttöjärjestelmä (NT)
Os2LibPath	DLL-kirjastojen sijainti
PATH	Hakupolku
PROCESSOR_ARCHITECTURE	Prosessorin tyyppi, esim. Intel = x86
PROCESSOR_IDENTIFIER	Prosessorin tyypin tarkemmat tiedot
PROCESSOR_LEVEL	Prosessorin taso, esim. Pentium Pro = 6
PROCESSOR_REVISION	Prosessorin tyypin tarkemmat tiedot
windir	Windows NT:n järjestelmähakemisto

Käyttäjäkohtaisia (*User Variables*) ovat oletuksena seuraavat:

Ympäristömuuttuja	Merkitys
TEMP	Väliaikaistiedostojen tallennushakemisto
TMP	Väliaikaistiedostojen tallennushakemisto

Ympäristömuuttujien muuttaminen tehdään seuraavasti:

1) Valitse **System Variables** tai **User Environment Variables**-ryhmästä muuttuja, jonka arvoa haluat muuttaa. Valitsemasi muuttujan nimi näkyy **Variable**-ruudussa ja sen arvo tulee **Value**-ruutuun. Voit myös napauttaa **Variable**-ruutua ja kirjoittaa sellaisen muuttujan nimen, jota ei ole luettelossa; lisäämäsi muuttujat liitetään tällöin nykyisen käyttäjäprofiilin ympäristömuuttujien luetteloon



3) Kirjoita **Value**-ruutuun uusi arvo muuttujalle

4) Valitse lopuksi **Set** ja **OK**.

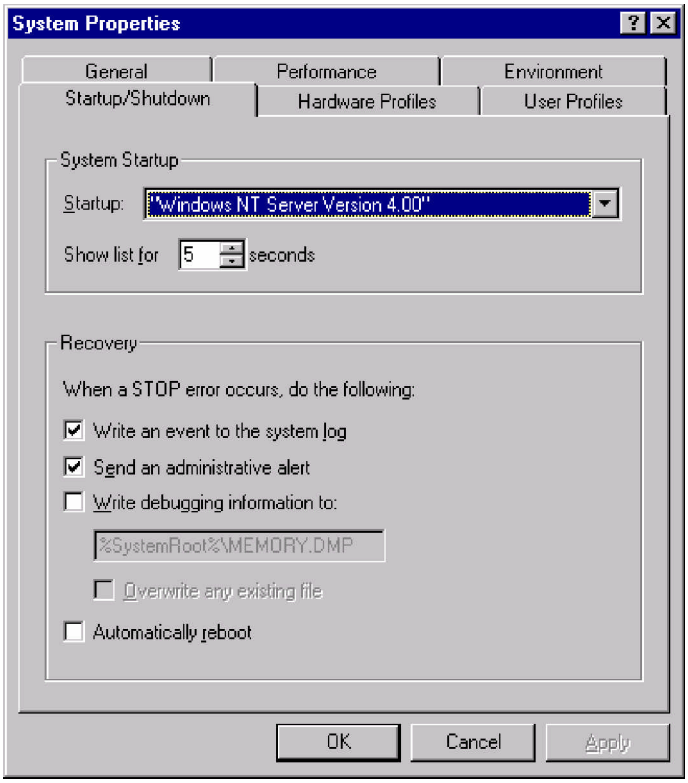
Voit **peruuttaa** kaikki tekemäsi muutokset valitsemalla **Cancel**, jolloin edelliset arvot palaavat käyttöön.

Käyttäjän ympäristömuuttujan poistaminen tehdään valitsemalla haluttu muuttuja **User Environment Variables**-ryhmästä ja valitsemalla **Delete**.

Muuttujiin tekemäsi muutokset tallentuvat heti rekisteritietokantaan (*Registry Database*), mutta ne **eivät vaikuta käynnissä oleviin ohjelmiin**. Muutokset tulevat voimaan vasta, kun mikro käynnistetään uudelleen.

Startup/Shutdown

Tässä välilehdessä käsitellään keskeisiä järjestelmän asetuksia; ota myös niihin liittyvät varoitukset vakavasti! Älä muuta asetuksia, jos et tarkalleen tiedä, mitä olet tekemässä!



Show list for seconds -asetuksella määritellään käynnistysvaiheen odotusaika, jonka jälkeen käynnistetään **Startup**-listasta valittu käyttöjärjestelmä. Palvelimessa kannattaa toki valita käynnistysviiveeksi vaikkapa **5** sekuntia, ennenkuin **Windows NT Server** käynnistetään. Asetusta ei kannata asettaa aivan nollaksi; tällöin et pääse käynnistämään Windows NT:tä perus-VGA-näytönohjaintilaan mahdollisena ongelmatilanteena.

Käynnistyslistan valinnat luetaan juurihakemistossa olevasta **piilotetusta BOOT.INI**-tiedostosta. Jos e.m. tiedosto tuhoutuu, Windows NT saattaa edelleen käynnistyä, jos Windows NT -käyttöjärjestelmän **lataustiedostot** ja **kernel** edelleen löytyvät oletushakemistosta, joka on käynnistysosion WINNT-hakemisto.

Huomattavaa:

- Jos listassa on MS-DOS-käynnistys, voit käyttää sitä vain, jos C:-aseman tiedostojärjestelmä on MS-DOS:in tukema FAT ja MS-DOS:in käynnistystiedostot ovat C:-asemassa. Jos käynnistät mikron MS-DOS-käynnistyslevykkeellä ja asennat MS-DOS:in C:lle MS-DOS:in SYS-komennolla, tuhoat samalla Windows NT:n käynnistyksen ja joudut tällöin asentamaan Windows NT:n uudelleen!

- NT-palvelimessa ei tällaista multiboottia tulisi missään tapauksessa olla!

- Jos haluat määrittää **vaihtoehtoisen käynnistyskäyttöjärjestelmän** Intel x86-prosessorilla varustetulle mikrolle, sinun on muokattava C:-aseman juurihakemistossa olevaa **piilotettua BOOT.INI**-tiedostoa. Voit muokata **BOOT.INI**-tiedostoa esimerkiksi **Notepadilla** tai **EDIT**-editorilla. Lisää vaihtoehtoisen järjestelmän nimi ja sijainti osaan **[operating systems]**. Kuvaus tulee **System**-valintaikkunan **Startup**-ruutuun

- Voit viitata **BOOT.INI**-tiedostossa lueteltuihin käyttöjärjestelmiin täysin vapaasti; on vain annettava käyttöjärjestelmän tiedostojen levyasema

- Samassa mikrossa voi useita eri Windows NT -asennuksia, kunhan ne sijaitsevat eri hakemistoissa.

Tässä mikrossa on sekä Windows NT 4.0 -työasema että -palvelin:

```
[boot loader]
timeout=30
default=scsi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV
[operating systems]
scsi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV="Win NT Srv"
scsi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV="Win NT Srv [VGA]" /basevi-
deo /sos
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Win NT Wksta"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Win NT Wksta [VGA]" /basevi-
deo /sos
```

Windows NT 4.0 -työasemasta että -palvelimesta voi olla mikrossa useita eri asennuksia, kunhan ne sijaitsevat jälleen eri hakemistoissa. Tässä mikrossa on sekä Windows NT 4.0 -työasema että kaksi Windows NT 4.0 -palvelinta (ATK-toimialueen *Domain Controller*- ja *Server*-tyyppinen palvelin) ja **BOOT.INI**:iin on kuvattu eri asennusten merkitys.

Kuvaus tulee näkyviin **Startup**-ruutuun:

```
[boot loader]
timeout=30
default=scsi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV
[operating systems]
scsi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV="ATK-domain/Server
scsi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV="ATK-domain/Server[VGA
mode]" /basevideo /sos
scsi(0)disk(0)rdisk(0)partition(1)\WINNT.BDC="ATK-domain/BDC"
scsi(0)disk(0)rdisk(0)partition(1)\WINNT.BDC="ATK-domain/BDC  [VGA
mode]" /basevideo /sos
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation [VGA
mode]" /basevideo /sos
```

Parametri **/basevideo /sos** käynnistää Windows NT:n perus-VGA-tilaan. Samalla nähdään luettelo ladattavista laiteohjaimista.

Jos töppäät **BOOT.INI**-asetukset NTFS-levyllä, anna NT-koneen käynnistyä ja ota yhteys C:-levyasemaan verkon kautta, esimerkiksi komennolla

NET USE Y: \\palvelin\C$

ja korjaa virheet **BOOT.INI**-tiedostossa.

Recovery mahdollistaa eräät automatisoidut toiminnot NT:n havaitessa **STOP**-tyyppisen virheen. Voit tehdä seuraavat valinnat:

- **Write an event to the system log** - virheen kirjaaminen tapahtumalokiin, jota voi tutkia **Event Viewerilla**

- **Send an administrative alert** - hälytys virhetilanteesta - kenelle, se määritellään **Server**-kuvakkeella **Alerts**-kohdassa

- **Write debugging information to** - tiedostonimi, jonne virhetilanteen tiedot tallennetaan - käytännössä koko keskusmuisti kirjoitetaan tiedostoon!

- **Overwrite any existing file** - kirjoitetaanko vanhan virhetiedoston päälle

- **Automatically reboot** - automaattinen uudelleenkäynnistys virhetilanteessa. Automaattinen uudelleenkäynnistys on hyödyllinen varsinkin palvelimissa, joiden lähistöllä ei vakinaisesti vaikuta mikrotukihenkilöitä ja jotka käyttäjän kannalta ovat staattisia , esimerkiksi WWW- tai FTP-palvelimia. Jos kuitenkin palvelimessa toimii useita prosesseja, niin sinänsä mitättömän tai toiminnan kannalta lähes tarpeettoman prosessin jumiutuminen kuitenkin käynnistää uudelleen koko palvelimen ja siten lopettaa myös kaikki edelleen toiminnassa olevat prosessit. Jos näiden prosessien käynnistys vastaavasti ei ole automaattinen, ne saattavat jäädä uudelleenkäynnistyksessä käynnistymättä!

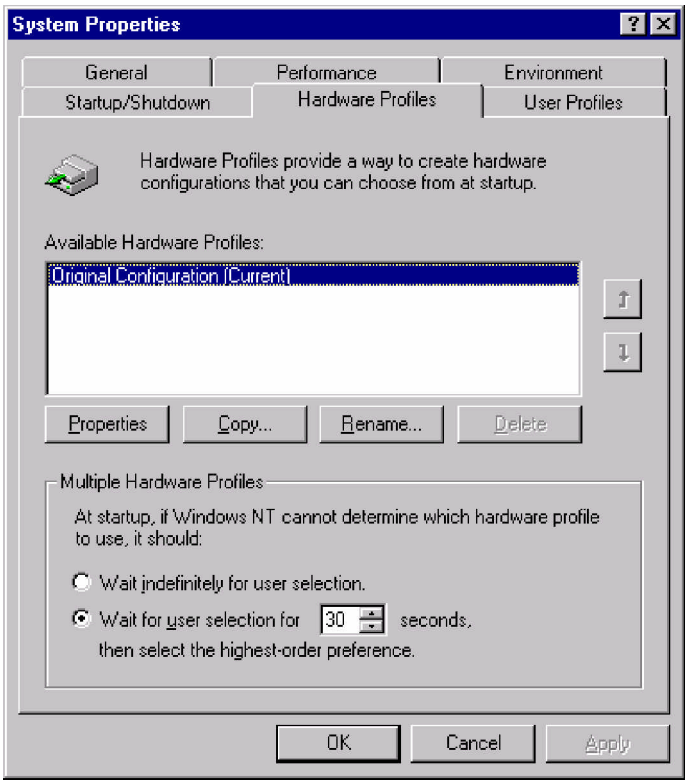
Jotta virheistä toipuminen toimisi luotettavasti, aseta sivutustiedosto samalle levyosiolle kuin **NTOSKRNL.EXE** ja sen koko suuremmaksi kuin keskusmuistin määrä.

Hardware Profiles

Hardware Profiles -välilehdessä voit luoda uusia kokoonpanoja - tämä voi olla hyödyllinen esimerkiksi kannettavissa mikroissa, jotka liitetään ns. **telakointiaseman** (*Docking Station*) avulla lähiverkkoon. Voit tehdä kopioita (**Copy**) tai nimetä uudelleen (**Rename**) laiteprofiilit.

Jos olet ottanut laitteistoprofiilit käyttöön, niin mikron käynnistyksessä kysytään mitä profiilia käytetään. Siksi voit määritellä oletuksena käytettävän listalle ensimmäiseksi, ja voit antaa odotusajan kohdassa **Wait for user selection**, jonka jälkeen listan ensimmäinen laitteistoprofiili otetaan käyttöön.

Eria asia sitten on, tarvitaanko tavallisissa palvelimissa ollenkaan laiteprofiileita!



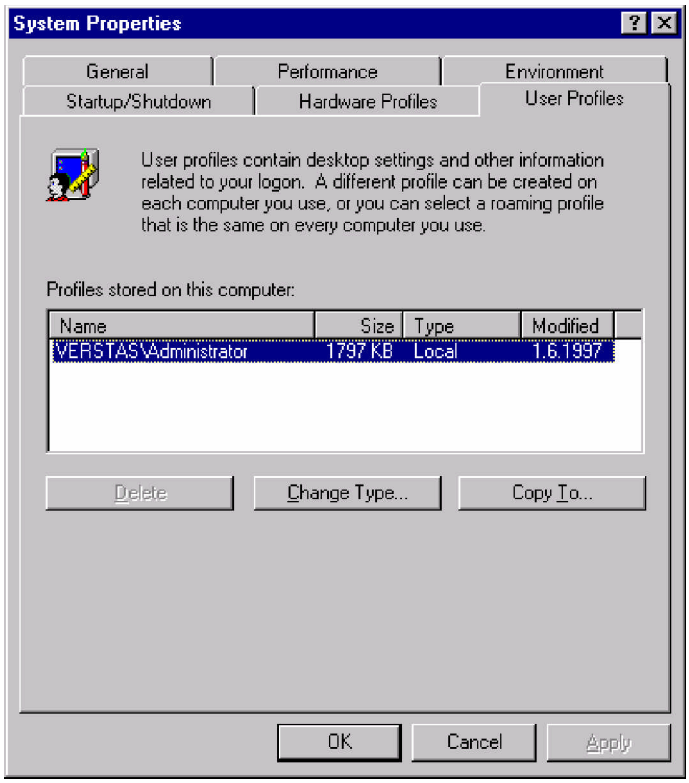
User Profiles

NT-koneessa **aiemmin** kirjautuneiden käyttäjien profiilit tyyppeineen näet **User Profiles**-välilehdessä. Toiminto on käytettävissä myös palvelimissa. Lue asiasta lisää **luvussa 5**.

Käyttäjän profiili voi olla paikallinen (**Local**), eli sijaita vain NT-koneen paikallisessa **Profiles**-järjestelmähakemistossa tai palvelimella sijaitseva (**Roaming**).

Jos haluat määritellä käyttäjälle **palvelimella sijaitsevan** (*Roaming*) profiilin, määritä käyttäjäprofiilin sijainti kirjoittamalla sen polku **User Manager for Domains**issa **User Profile Path** -ruutuun; polun on oltava **verkkopolku** annettuna UNC-nimellä, esimerkiksi **\\V1\PROFILES\JKI**.

Lisäksi mahdollisen työasemassa jo sijaitseva **paikallisen** (*Local*) profiilin tyyppi ja sijainti on muutettava **User Profiles**-välilehdessä **Change Type**- ja **Copy To**-painikkeilla. Voit myös poistaa profiilin **Delete**llä, jos et ole tällä hetkellä kirjautunut käyttäjätunnuksella, joka käyttää a.o. profiilia.



Tape Devices

Windows NT:ssä käytetään nauhavarmistuslaitteista nimitystä **nauhalaite** (*Tape Device*).

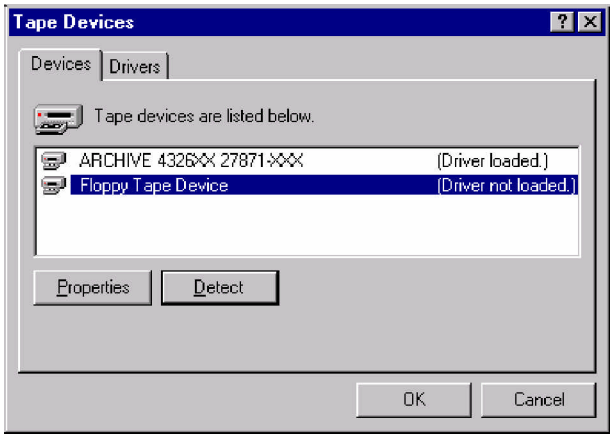
Tape Devicesin avulla asennetaan nauhavarmistuslaitteiden laiteohjaimet, niiden asentaminen ja asetukset. **Devices**-välilehdestä näet asennetut laitteet (fyysiset ohjaimet) ja **Drivers**-välilehdestä näet asennetut laiteohjaimet eli ajurit asetuksineen.

Windows NT tukee useita eri nauhalaitteita, niinpä NT-koneeseen voi olla samanaikaisesti asennettuna useita eri nauha-asemia, mutta varmuuskopiointiin voi käyttää vain yhtä asemaa samanaikaisesti kerrallaan. Windows NT:n **Backup**-ohjelmalla voit tallentaa sekä paikallisten että verkkoasemien tiedostoja nauha-asemaan.

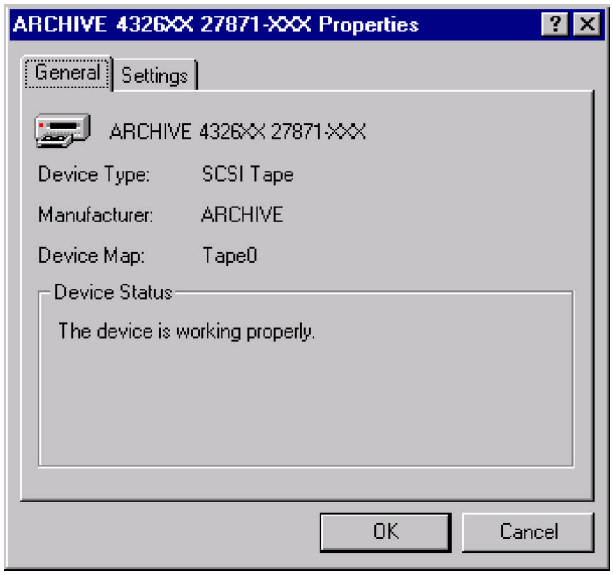
Nauhalaitteita on käsitelty myös **luvussa 11**.

Devices

Devices-välilehdestä nähdään asennetut nauhalaitteet. Tässä esimerkin palvelimessa on käytettävissä Archiven 4 mm DAT-nauhuri.

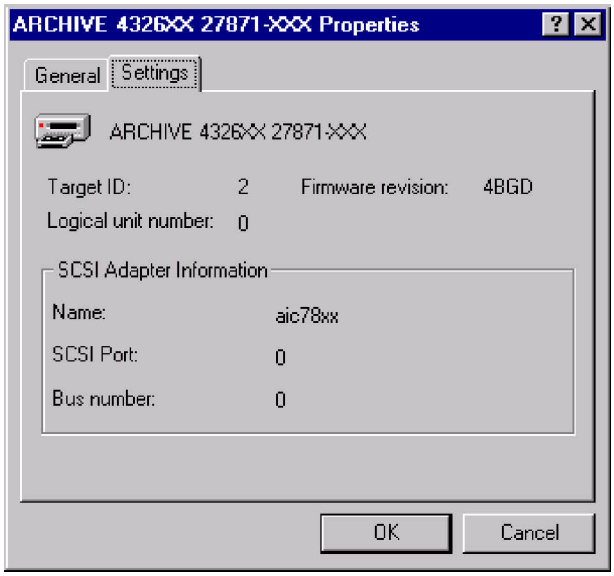


Jos laite on juuri asennettu, voit painaa **Detect** ja se yritetään tunnistaa. Valitsemalla laite ja painamalla **Properties** saadaan lisätietoja asennetusta laitteesta.



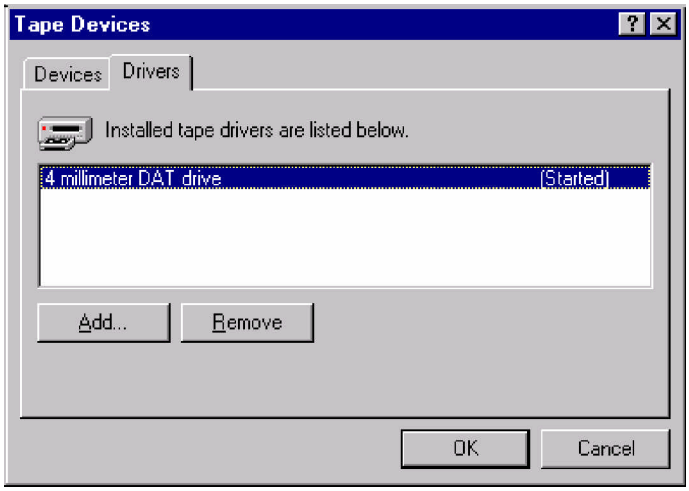
General-välilehti kertoo laitteen tyypin (**SCSI Tape**) ja valmistajan (**Manufaturer**) sekä toimintatilan (**Device Status**), jonka mukaan laite toimii ja on käytettävissä.

Settings-välilehti kertoo mm. SCSI ID:n (**2**), portin, väylän ja SCSI-ohjaimen (**aic78xx**):



Drivers

Drivers-välilehdellä voidaan lisätä (**Add**) tai poistaa (**Remove**) asennettuja laiteohjaimia. Samalla nähdään laiteohjaimen tila (**Started**).

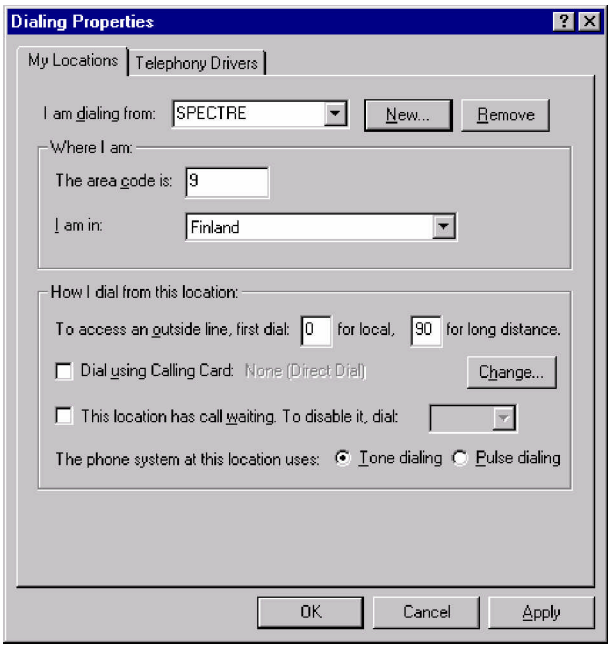


Telephony

Telephony asettaa puhelinohjaimet sekä soiton asetukset.

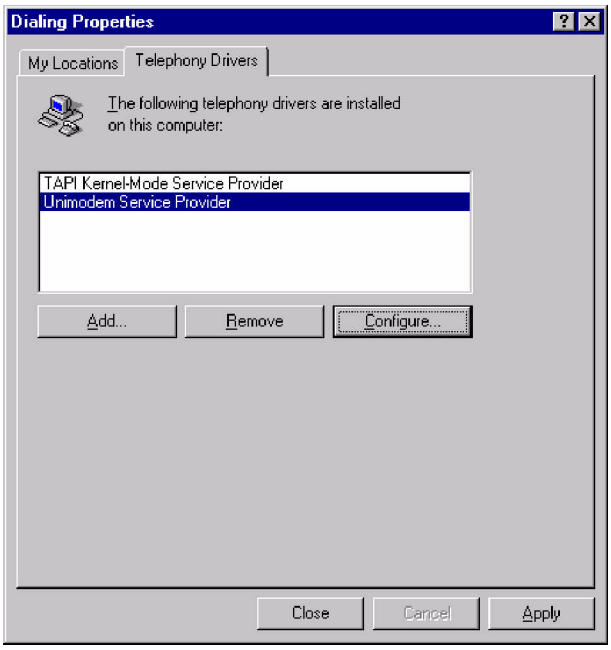
My Locations

My Locations määrittelevät modeeminkäyttöön liittyvät numeronvalintasetukset. Kohtaan **I am dialing from** voit antaa sijainnin nimen tai luoda uuden painikkeella **New** tai poistaa asetukset painikkeella **Remove**. Voit määritellä käyttöön puhelukortin (**Calling Card**) ja koputustoiminnon (**call waiting**). Valitse tarvittaessa oikea valintamenetelmä: äänivalinta (**Tone dialing**) tai pulssivalinta (**Pulse dialing**).



Telephony Drivers

Telephony Drivers-välilehdellä määritellään puhelinohjaimet. Jos valitset **Configure**, siirrytään modeemien asetuksiin. Katso **Modems** aiemmin tässä luvussa.



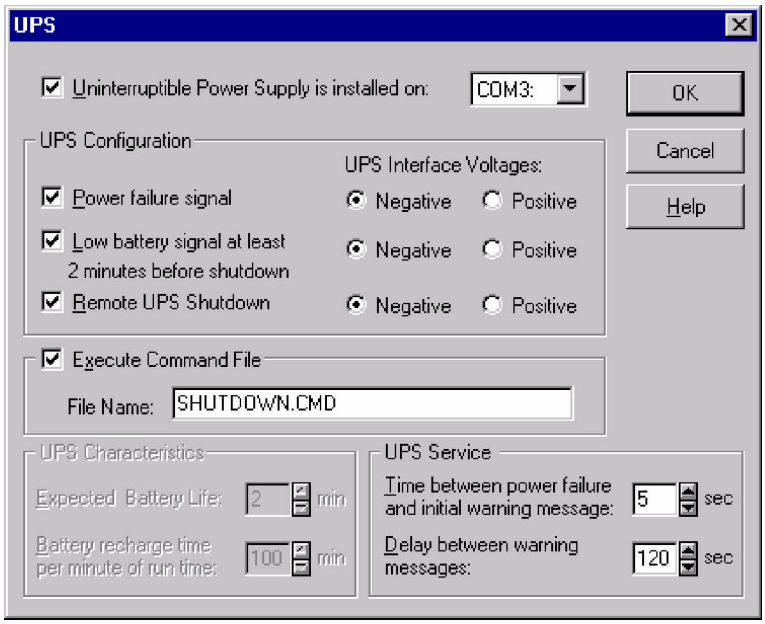
UPS

UPS-palvelulla annetaan **keskeytymättömän virransyötön** (*Uninterruptible Power Supply*) asetukset, joka varmistaa järjestelmän sammuttamisen oikein virtakatkoksen aikana.

UPS-palvelun vaihtoehdot riippuvat järjestelmään asennetusta UPS-laitteistosta.

UPS-palveluiden asentaminen tehdään seuraavasti:

1) Valitse UPS-valintaikkunasta **Uninterruptible Power Supply is installed on** sarjaportti, johon UPS-laite on liitetty.



Muut vaihtoehdot ovat käytettävissä tämän jälkeen:

- Jos UPS-laite voi lähettää sanoman virtakatkoksen sattuessa, valitse **Power failure Signal**; asetus vastaa UPS:n sarjaportin **CTS** (*Clear-To-Send*)-signaalia

- Jos UPS-laite voi lähettää merkkiäänen akun latauksen vähetessä, valitse **Low Battery Signal** - asetus vastaa UPS:n sarjaportin **DCD** (*Data-Carrier-Ddetect*) -signaalia

- Jos UPS-laite akku voi vastaanottaa UPS-palvelulta sammutussignaalin, sinun on määritettävä oikea liittymän jännite, vaikka et ottaisi etäsammutusta käyttöön; jos jännite on väärä, eräät UPS-laitteet voivat sammuttaa tietokoneen heti virtakatkoksen sattuessa. Valitse vaihtoehdon **Remote UPS Shutdown** vierestä UPS-liittymän jännitteeksi positiivinen (**Positive**) tai negatiivinen (**Negative**). Asetus vastaa UPS:n sarjaportin **DTR** (*Data-Terminal-Ready*) -signaalia

- Määritä jokaiselle **UPS Interface Voltages** -ryhmän vaihtoehdolle UPS-liittymän jännitteeksi positiivinen (**Positive**) tai negatiivinen (**Negative**); se määrittää, miten UPS-laite kommunikoi UPS-palvelun kanssa. Lisätietoja asetuksista on UPS-laitteen oppaissa

- Anna akun odotettu kesto ruutuun **Expected Battery Time** aika minuutteina, jonka järjestelmä voi toimia UPS:in akun varassa. Arvot ovat **2 - 720 minuuttia**, oletusarvo on **2 minuuttia**

- Anna **Battery Recharge Time**-ruutuun aika minuutteina jonka verran akkua on ladattava jokaista **käyttöminuuttia** kohti: sallitut arvot ovat **1 - 250 minuuttia** ja oletusarvo on **100 minuuttia** jokaista **käyttöminuuttia** kohti

- Anna **Time between power failure and initial warning message**-ruutuun aika sekunteina joka kuluu sähkökatkon ja ensimmäisen käyttäjille lähetettävän sanoman välillä: arvot ovat **0 - 120 sekuntia** ja oletusarvo on **5 sekuntia**

- Kirjoita **Delay between warning messages** -ruutuun aika sekunteina aika joka kuluu sähkökatkosta ilmoittavan viestin ja työaseman käytön lopettamiskehotuksen välillä. Sallitut arvot

ovat **5 - 300 sekuntia** ja oletusarvo on **120 sekuntia**

2) Valitse lopuksi **OK**.

Valitse Ohjauspaneelista **Services**-kuvake ja sitten **UPS**. Voit aloittaa tai lopettaa palvelun ja määrittää, käynnistyykö palvelu automaattisesti, kun käynnistät NT:n.

Käytön voit lopettaa poistamalla UPS-valintaikkunassa vaihtoehdon **Uninterruptible Power Supply is installed on** valinta.

4. KÄYTTÖLIITTYMÄ

Windows NT 4.0:n käyttöliittymää on käsitelty Windows NT 4.0 Tehokäyttäjän Opas Osa 1:ssä.

Tässä luvussa käsitellään käyttöliittymää järjestelmänhallinnan näkökulmasta.

Verkkotietokoneiden (*Network Computer*, NC) puristuksessa Microsoft on tuomassa **Zero Administration Windows** (ZAW)-konseptia helpottaakseen PC-ympäristön hallintaa. Windows -ympäristöstä - varsinkin Windows NT 4.0 -ympäristöstä - saadaan muutamalla tempulla varsin hyvin suojattu ja helposti ylläpidettävä järjestelmä. Itse asiassa ZAW hyödyntää vahvasti jo olemassa olevia (mutta huonosti tunnettuja) Windows NT:n suojausmenetelmiä. Katso luvusta **11** ohjeita, miten rakennetaan **Kioski-työasema**.

Käyttämällä **User Manager for Domains**in asetuksia, **NTFS**-suojauksia, **Policy Editor**ia ja **rekisterieditoria** voidaan rakentaa käyttäjäystävällinen, mutta hyvin hallittu työasema- ja verkkoympäristö.

Suojaukset

Käyttöliittymän suojaukset on helpointa rakentaa Policy Editorin järjestelmäkäytäntöjen avulla (ks. Luku **5**). Voit myös käyttää suoraan rekisterieditoria muokataksesi käyttöliittymän asetuksia.

Tyypillisesti suojauksilla on kaksi tarkoitusta:

- Sallia käyttäjälle pääsy vain sallittuihin resursseihin
- Estää käyttäjän pääsy kiellettyihin resursseihin.

Ensimmäinen voidaan toteuttaa **Policy Editor**illa - käyttäjä ei edes näe muuta kuin sallittuja resursseja (hakemistot, tiedostot, pikakuvakkeet). Tässä voidaan käyttää apuna myös kirjauskomentojonoja (*Logon Scripts*).

Toinen voidaan toteuttaa NTFS:n ja **User Manager for Domains**in avulla.

Shell

Kuori (Shell) on itse asiassa **Explore.exe**-ohjelmatiedosto. Käyttöliittymäksi saa jonkin toisenkin ohjelmatiedoston, esimerkiksi Internet Explorerin. (Katso luvusta 11 Kioski-työasema).

Rekisterin asetukset

Tyypillinen rekisterin asetus on tuoda käyttöliittymä näyttöön, vasta kun kirjauskomentojono on suoritettu. Oletus on **0** (käyttöliittymä tulee heti käyttöön). Jos muutat asetuksen arvoon **1**, odotetaan komentojonon päättymistä. Sijainti rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**RunLogonScriptSync**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei voimassa (oletus), 1 voimassa**

HKEY_LOCAL_MACHINE:n asetus vaikuttaa kaikkiin työaseman käyttäjiin, **HKEY_CURRENT_USER** vain kirjautuneeseen.

Windows NT:ssä ei ole vanhaa kunnon **Autoexec.bat**:ia, mutta voit kuitenkin määritellä käyttäjän kirjautuessa automaattisesti käynnistettävät ohjelmat rekisteriin:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**UserInit**
Tyyppi	**REG_SZ**
Arvo	**Oletus: USERINIT,NDDEAGNT.EXE**

Lisää ohjelmatiedoston (EXE) nimi merkkijonoon. Anna tarvittaessa polku.

Samasta avaimesta löytyvä **System** ajaa sovellukset kun järjestelmä käynnistyy käyttäen järjestelmän oikeuksia. Oletuksena ajetaan **lsass.-exe**. Älä poista oletusasetuksia!

Käyttöliittymän muokkaaminen

Internet Explorer 4.0 tulee muuttamaan työpöytää melkoisesti. On syytä toivoa, että mukana tulee riittävästi työkaluja käyttöliittymän ja järjestelmän suojaamiseen!

Rekisterin asetukset käyttäjän kirjautumisessa

Rekisteristä löytyy useitakin asetuksia käyttöliittymän muokkaamiseen. Useimpia hyödyllisistä asetuksista voit tehdä Policy Editorin avulla. Seuraavat asetukset näkyvät käyttäjän kirjautumisen yhteydessä (ks. myös luku 11, jossa on käsitelty kirjautumista automaattisesti).

Voit esimerkiksi lisätä tekstin **Begin Logon**-, **Logon Information**-, **Workstation Locked**- ja **Unlock Workstation**-ikkunoihin:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**Winlogon**
Tyyppi	**REG_SZ**
Arvo	**Max 256 merkkiä pitkä merkkijono - arvo on lisättävä**

Kirjautumisikkunan teksti:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**LogonPrompt**
Tyyppi	**REG_SZ**
Arvo	**Max 256 merkkiä pitkä merkkijono - oletus: Enter a user name and password that is valid for this system.**

Käyttöympäristön asetuksia

Asetuksia, jotka ovat hyödyllisiä - vaikka eivät liitykään kirjautumiseen - ovat seuraavat. CD-ROM-levyjen automaattinen toiston voi kytkeä pois rekisteristä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Cdrom**
Nimi	**Autorun**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei automaattista käynnistystä, 1 - automaattinen käynnistys**

Muuttamalla arvon 0:ksi ei levyjä käynnistetä automaattisesti.

Käynnistä (Start)-painikkeen viive asetetaan:

Polku	**HKEY_USERS\.DEFAULT**
Avain	**Desktop**
Nimi	**MenuShowDelay**
Tyyppi	**REG_SZ**
Arvo	**Viive millisekunteina (oletus 400)**

Tämä muuttaa oletuskäyttäjän asetuksia - kirjautuneen käyttäjän asetus löytyy **HKEY_CURRENT_USER**ista.

Komentorivin merkkien täydentäminen asetetaan:

Polku	**HKEY_USERS\.DEFAULT**
Avain	**Software\Microsoft\Command Processor**
Nimi	**CompletionChar**
Tyyppi	**REG_DWORD**
Arvo	**0 (oletus), 9 - täydennys**

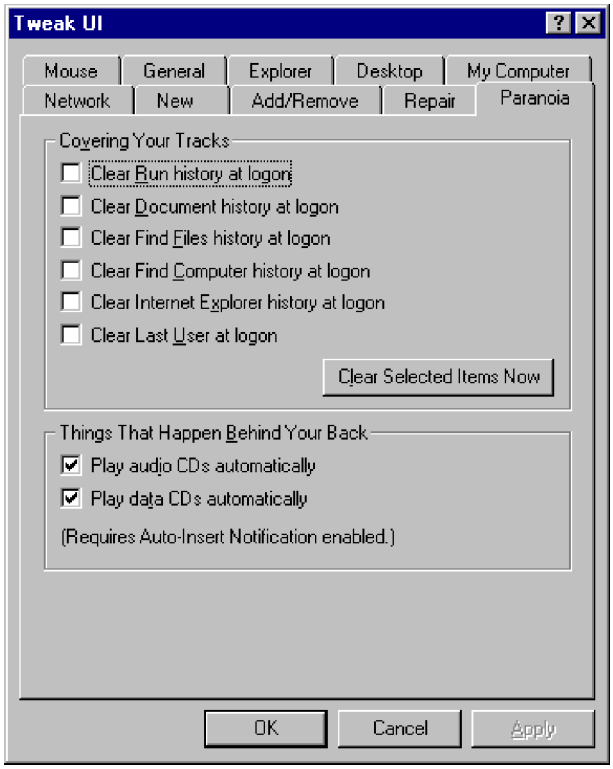
Tämä muuttaa oletuskäyttäjän asetuksia - kirjautuneen käyttäjän asetus tuksia - kirjautuneen käyttäjän asetus löytyy **HKEY_CURRENT_USER**ista.

Asetuksen huomaat komentorivillä kirjoittaessasi komennon alkuosan. Kun painat tabulaattoria (sarkainta), komento täydentyy ensimmäisellä löytyvällä tiedostonimellä, hakemistonimellä jne.

Käyttöliittymän apuohjelmat

Käyttöliittymän apuohjelmista yksi monipuolisimmista lienee **PowerToys** (alunperin Windows 95-apuohjelmistopaketti) ja sen **Tweak UI**, jolla voit muokata ympäristöä varsin mukavasti.

Pääkäyttäjille löytyy esimerkiksi automaattisen kirjautumisen asetukset ja työpöydän sekä järjestelmätiedostojen korjaus.



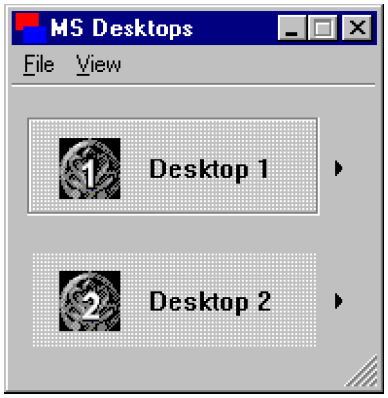
Ohjelmistopaketti löytyy Microsoftin WWW-palvelimelta sekä Windows NT 4.0 Resource Kiteistä.

Resource Kitin apuohjelmia

Edellämainittu PowerToys tulee Windows NT 4.0 Resource Kitin mukana, mutta niin myös seuraavat lyhyesti esitellyt käyttöliittymän hallintaan tarkoitetut apuohjelmat.

Desktops

Desktops on apuohjelma, jolla saadaan käyttöön useampi virtuaalinen työpöytä. Niiden välillä siirrytään **Ctrl+funktionäppäin** -yhdistelmillä.

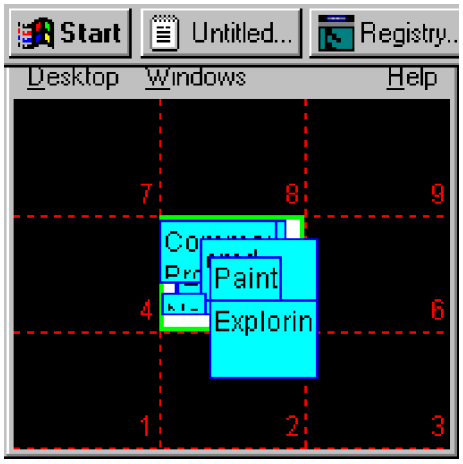


Netcons

Netcons on apuohjelma, jolla pääset toisen NT-koneen komentoriville valitsemalla kohteen kaksoisnapautuksella!

Topdesk

Topdesk mahdollistaa näytön jatkamisen näytön reunan yli.



Vdesk

Myös **Vdesk** mahdollistaa myös useita työpöytiä - itse asiassa mahdollistaa jopa käyttäjän kirjautumisen toisessa työpöydässä!

5. KÄYTTÄJIEN HALLINTA

Käyttäjien hallinta laajassa Windows NT -verkossa on yksi haasteellisimmista asioista. Koska eritasoiset oikeudet jaettuihin resursseihin yleensä eritellään käyttäjäryhmien avulla, huonosti hallitut käyttäjätunnukset ja -ryhmät aiheuttavat taatusti melkoisesti ongelmia.

Käyttäjien hallinta **ei** kuitenkaan missään tapauksessa ole *ylivoimaisen* hankala tehtävä. Seuraavaksi selitetään käyttäjien hallinnan pääperiaatteet.

Käyttäjätunnuksia hallitaan seuraavilla NT:n työkaluilla:

- **User Manager for Domains** - Windows NT -palvelimissa
- **Käyttäjien hallinta** (User Manager) - Windows NT -työasemassa
- **Käyttäjien profiilit** - Windows NT -työasemissa
- **System Policy Editor** - Lisäasetuksia Windows NT -työasemiin
- **Komentorivin NET-komennot**
- **Resource Kit** - Useita eri työkaluja, **DELPROF**, **IFMEMBER** jne
- **Muut apuohjelmat** - **DUMPACL** jne.

Työryhmän ja toimialueen käyttäjien hallinta

Keskeisiä kysymyksiä käyttäjien hallinnassa ovat seuraavat:

- Missä käyttäjätunnus on määritelty?
- Mihin ryhmiin käyttäjätunnus kuuluu?
- Mitkä ovat kyseisen käyttäjätunnuksen ja -ryhmän oikeudet kohteessa?

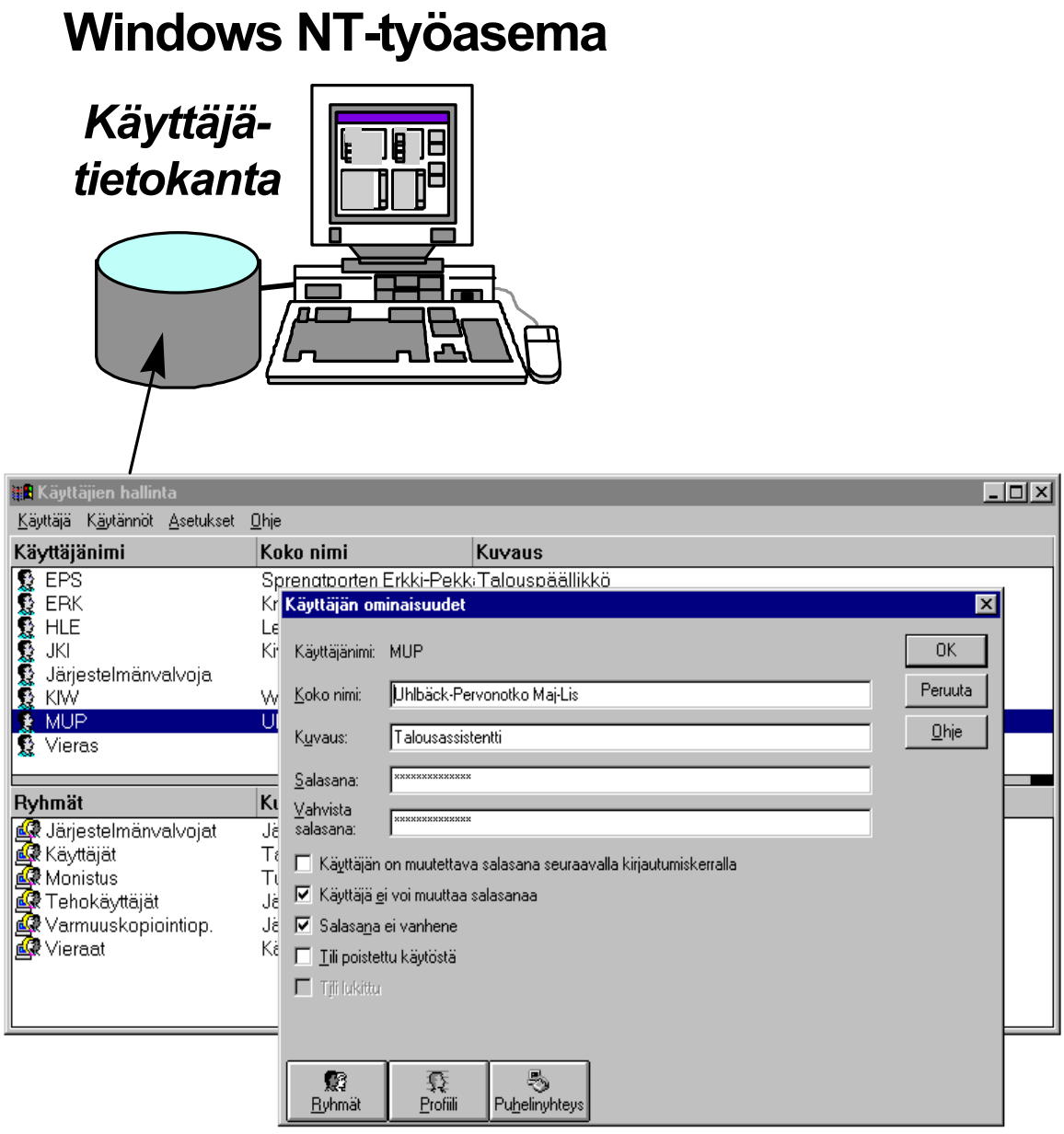
Käyttäjien hallinnoinnin keskeiset työkalut Windows NT:ssä ovat kaksi käyttäjien hallintaohjelmaa, **Käyttäjien hallinta** (User Manager) ja **Toimialueen käyttäjien hallinta** (User Manager for Domains).

Koska **Toimialueen käyttäjien hallinta** (User Manager for Domains)-suomennus on ollut käytettävissä aiemmin suomennetussa NT 3.x-palvelinversiossa, eikä Windows NT 4.0 Serveriä suomenneta, niin selvyyden vuoksi jatkossa **User Manager for Domains** tarkoittaa Windows NT 4.0-palvelimen mukana tulevaa käyttäjien hallintaohjelmaa.

Windows NT -työasema

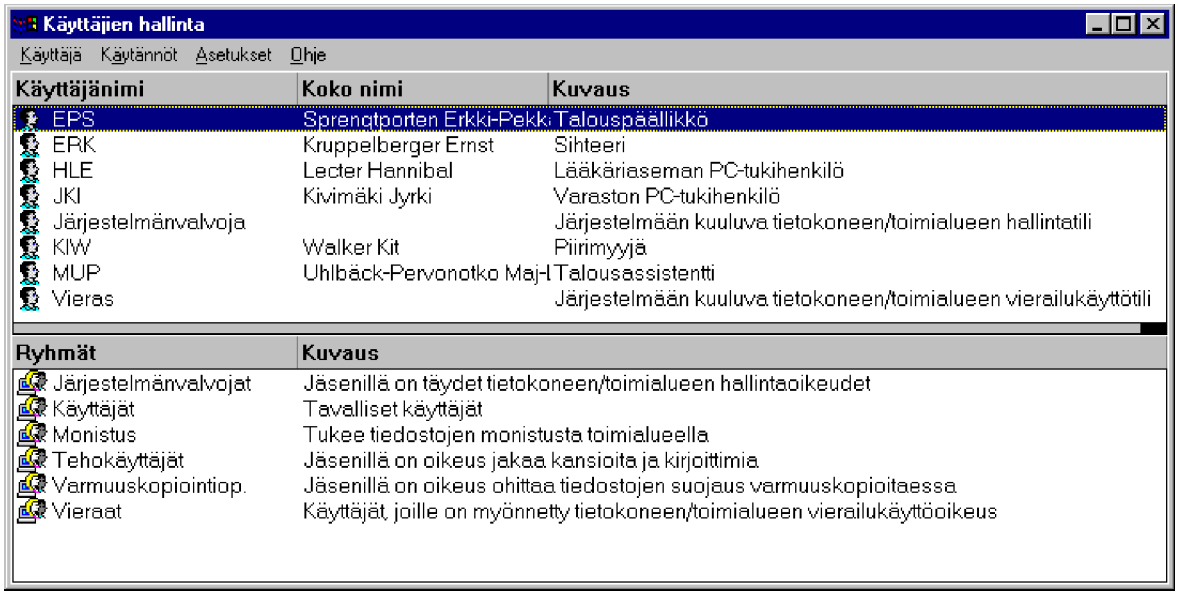
Jokaisessa NT-työasemassa on aina oma **Käyttäjien hallintansa** (User Manager), jolla voi hallita **vain** kyseisen Windows NT -työaseman **omaa paikallista käyttäjätietokantaa**.

Tätä työasemakohtaista käyttäjätietokantaa **ei** voi poistaa tai kopioida. Siitä voi kuitenkin ottaa nauhavarmistuksen Windows NT:n omalla nauhavarmistusohjelmalla.



Käyttäjien hallinta (User Manager) on apuohjelma, jonka avulla hallitaan **NT-työasemien** käyttäjätunnuksia ja suojausasetuksia. Käyttäjien hallinnan avulla voi tehdä seuraavat toimet:

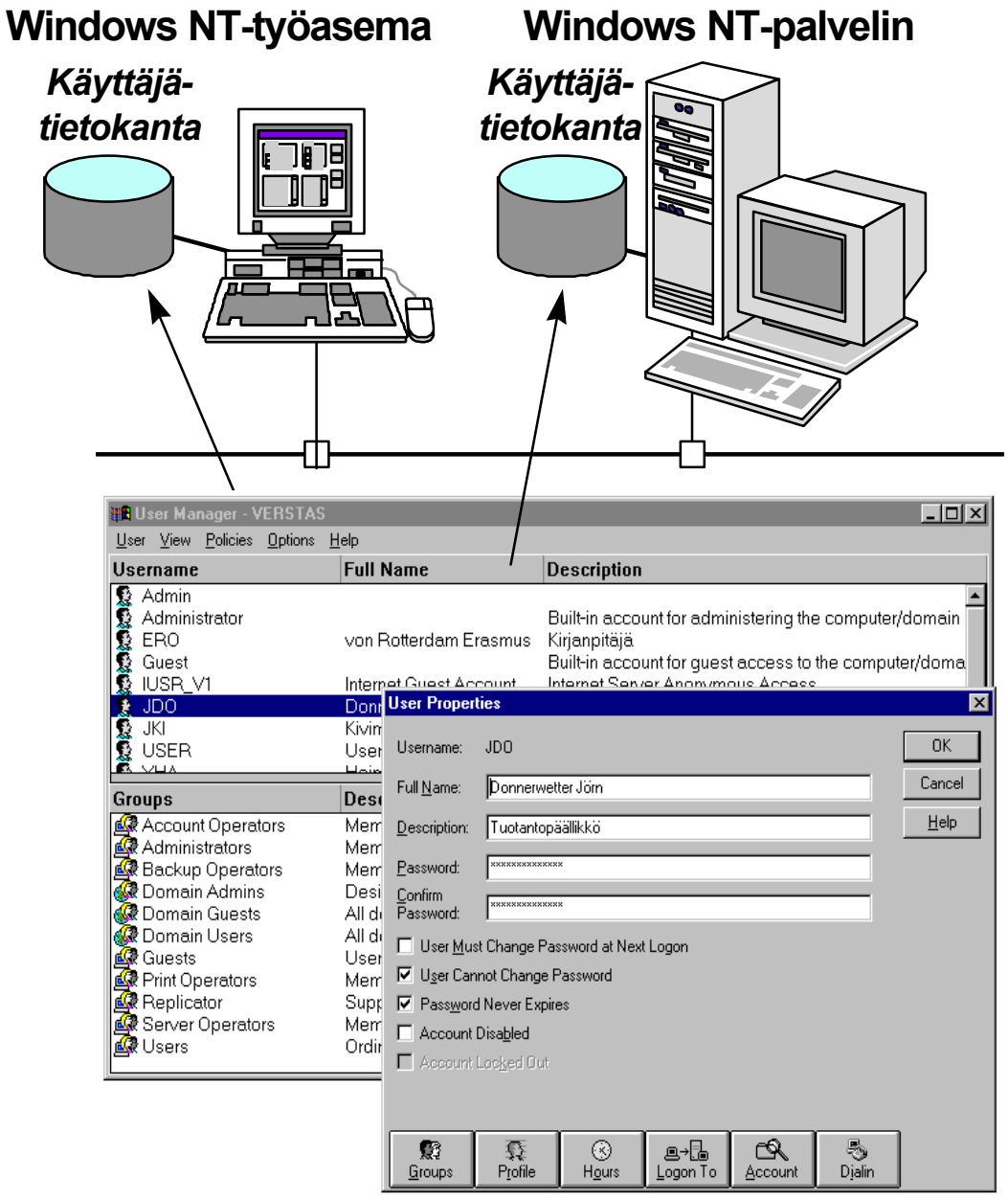
- luoda ja hallita työaseman käyttäjätunnuksia
- luoda ja hallita työaseman käyttäjäryhmiä
- hallita työaseman suojauskäytäntöjä.



Windows NT -toimialue

Windows NT 4.0-palvelimien mukana tulee **User Manager for Domains**, jolla voi hallita Windows NT -palvelimen muodostaman **toimialueen** (*domain*) **keskitettyä käyttäjätietokantaa** kuten myös minkä tahansa **Windows NT -työaseman käyttäjätietokantaa** (riippuen käytetyn käyttäjätunnuksen oikeuksista kyseisessä NT-työasemassa). Pääasiassa **User Manager for Domainsia** käytetään toimialueen keskitetysti hallittujen käyttäjätunnusten hallinnointiin.

Toimialueen keskitettyä käyttäjätietokantaa ei voi poistaa tai kopioida, mutta siitäkin voi ottaa nauhavarmistuksen Windows NT:n omalla nauhavarmistusohjelmalla.

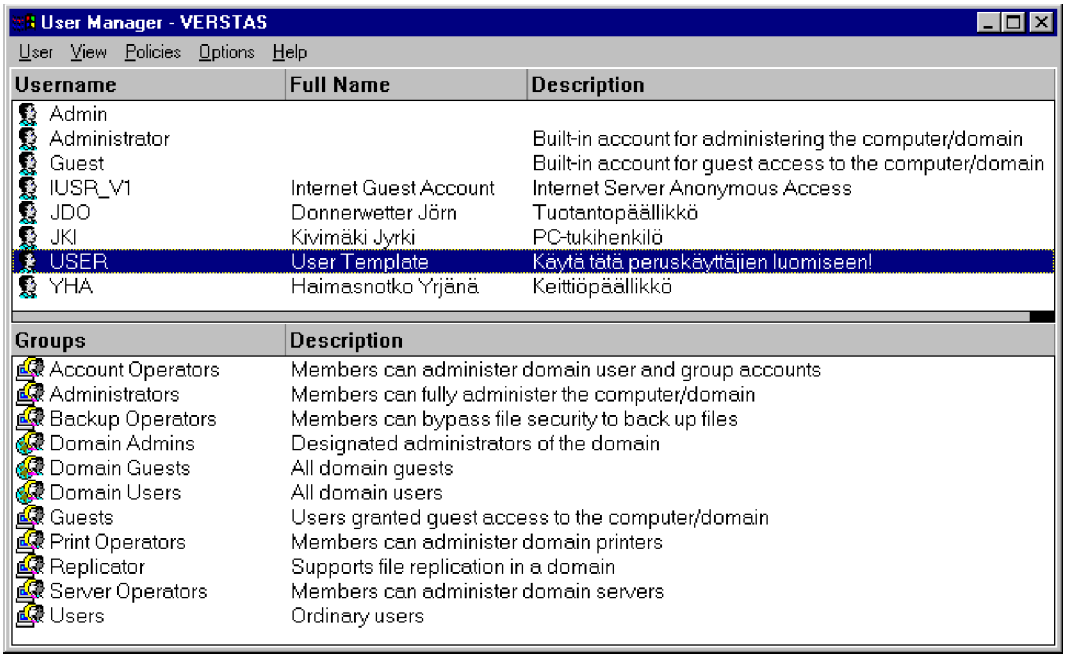


User Manager for Domains on työaseman käyttäjien hallintaohjelmaa laajempi, toimialueen kattava käyttäjien hallintaväline, jonka avulla voit:

- valita hallittavan toimialueen, palvelimen tai työaseman
- luoda ja hallita toimialueen käyttäjätunnuksia
- luoda ja hallita toimialueen paikallisia ja yleisiä ryhmiä
- hallita suojauskäytäntöjä
- hallita luottosuhteita (*Trusted relationships*)
- hallita **MS Exchangen**, **MS SQL Serverin** ja **MS Internet Information Serverin** käyttäjätunnuksia.

Voit vaihtaa toimialuetta tai valita kohteeksi yksittäisen Windows NT -työaseman valitsemalla **User | Select Domain**. Anna tällöin kyseisen toimialueen tai työaseman nimi, esimerkiksi **VERSTAS** tai **\\WS2**.

User Manager for Domainsin työasemaversio (Windows NT 4.0 ja Windows 95) tulee myös Windows NT 4.0 Serverin CD-ROM:illa.

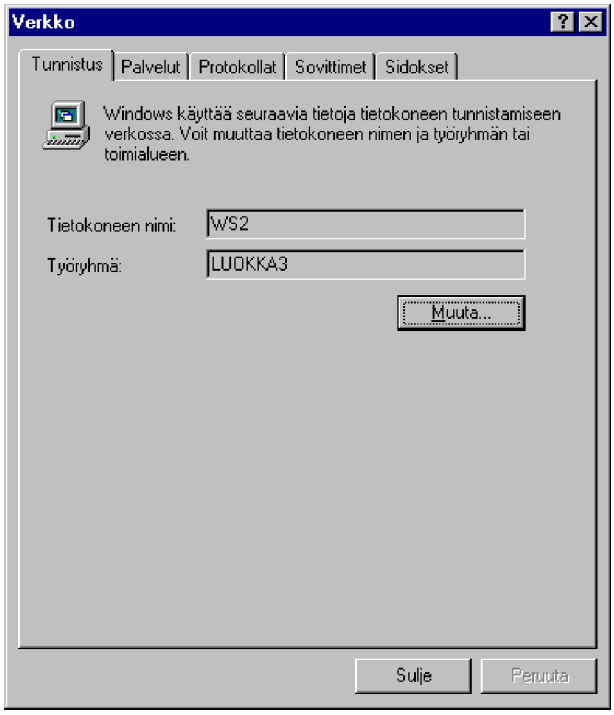


Työryhmä ja toimialue

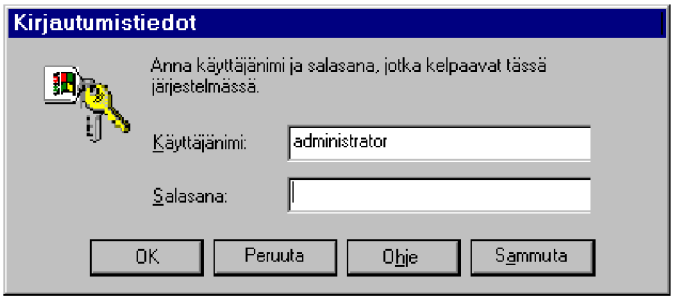
Milloin sitten käytetään kumpaakin näistä käyttäjien hallintaohjelmista?

Jos Windows NT -työasema kuuluu työryhmään (sen voit tarkistaa Ohjauspaneelin **Verkko** (Network)-kuvakkeella, käyttäjä voi kirjautua **vain työaseman käyttäjäksi ja vain työaseman paikallisilla käyttäjätunnuksilla**.

Tämä työasema kuuluu **työryhmään** (Workgroup) **LUOKKA3**:



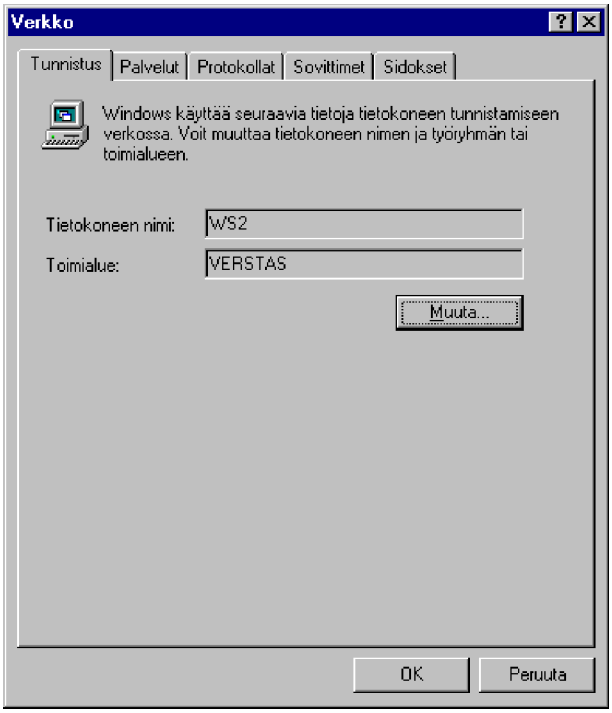
Työryhmään kuulumisen huomaat myös siitä, että työaseman kirjautumisen yhteydessä kysytään **vain** käyttäjätunnus ja salasana.



Ainoa tapa hallita työaseman käyttäjätietokantaa on tällöin **Käyttäjien hallinta** (User Manager). Käyttäjätunnukset on siis hallittava **erikseen** jokaisen työaseman käyttäjätietokannassa!

Etähallinta on mahdollista **Käyttäjien hallinnassa** (User Manager), jos toisessa työasemassa (tai palvelimessa) kirjaudutaan sellaisella käyttäjätunnuksella ja salasanalla, joka **hallittavassa kohdetyöasemassa** kuuluu työaseman paikalliseen **Järjestelmänvalvojat** (Administrators)-ryhmään.

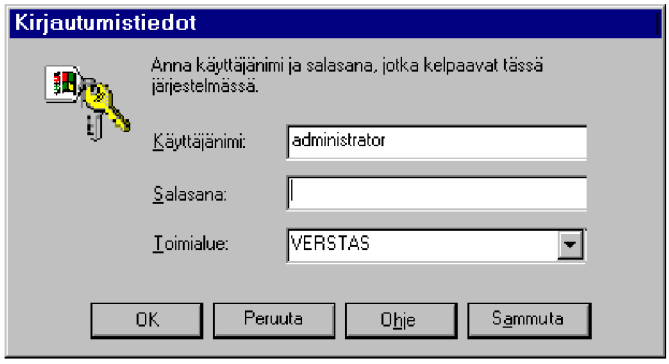
Jos Windows NT -työasema kuuluu toimialueelle (ja senkin voit tarkistaa Ohjauspaneelin **Verkko** (Network)-kuvakkeella), käyttäjä voi kirjautua **joko** työaseman paikallisilla käyttäjätunnuksilla tai **toimialueen yleisillä käyttäjätunnuksilla**. Tämä työasema kuuluu toimialueelle (*Domain*) **VERSTAS**.



Tämän huomaat myös siitä, että työaseman kirjautumisen yhteydessä kysytään **toimialueen** (Domain) käyttäjätunnus ja salasana. Ole tarkkana! Voit valita toimialuelistasta **myös** kyseisen NT-työaseman tunnuksen - tällöin voit kirjautua käyttäjäksi **vain** kyseisen NT-työaseman paikallisilla käyttäjätunnuksilla!

Jos toimialueelta (johon NT-työasema kuuluu) on luottosuhde toiseen toimialueeseen, käyttäjä voi kirjautua myös kyseisen luotetun toimialueen käyttäjätunnuksella. Vaihdoehdot näkyvät toimialuelistasta. Tällöin

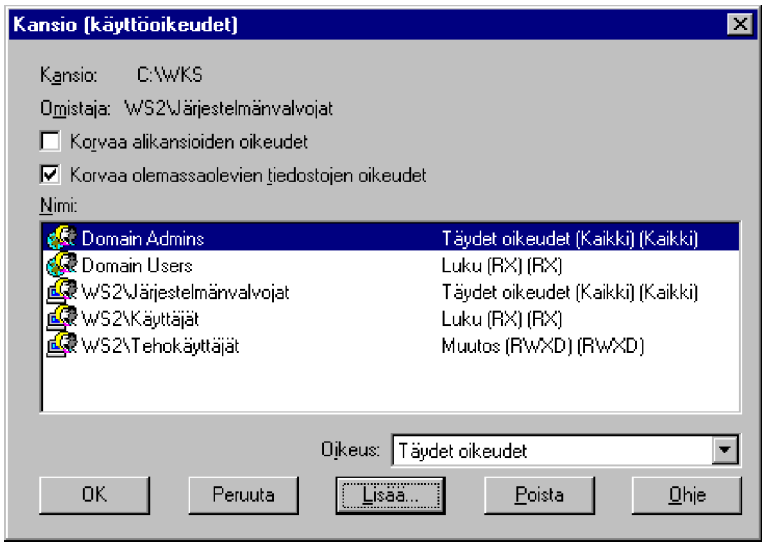
hänen oikeutensa oman toimialueen resursseihin määräytyvät sen mukaan, miten ryhmäjäsenyydet toimialueiden välillä on järjestetty.



Toimialueen käyttäjätietokantaa hallitaan **User Manager for Domainsilla**. Toimialueen muodostamiseen tarvitaan **aina** vähintään yksi Windows NT -palvelin, jonka tyyppi on **toimialueen ensisijainen ohjauskone**, **Primary Domain Controller**. Tällöin käyttäjätunnukset voidaan **keskitetysti** hallinnoida kyseisen palvelimen käyttäjätietokannassa.

Käyttäjätunnuksen sijainnin (ts. käyttäjätietokannan sijainnin) tunnistat **useimmiten** käyttäjätunnuksen edessä olevasta nimestä: esimerkiksi **WS2\Käyttäjät** viittaa **NT-työaseman** nimeltä **WS2** käyttäjäryhmään nimeltä **Käyttäjät**.

Käyttäjäryhmät, jotka alkavat etuliitteellä **Toimialueen...** (Domain), ovat **aina** toimialueella määriteltyjä käyttäjätunnuksia. Niinpä tässä esimerkissä työasemassa nimeltä WS2 **Domain Admins** ja **Domain Users** ovat toimialueen käyttäjäryhmiä ja **WS2**-merkillä alkavat ryhmät NT-työasemassa **WS2** määriteltyjä käyttäjäryhmiä.



Esimerkin toimialueen englanninkielisessä PDC:ssä ja suomenkielisessä työasemassa eri ryhmien nimet ovat kyseisellä kielellä.

Oletuskäyttäjätunnukset ja -ryhmät

Primary Domain Controllerin (PDC), **Stand-Alone Serverin** ja **NT-työaseman** asennuksessa syntyvät oletuskäyttäjätunnukset ja -ryhmät ovat seuraavat:

Oletuskäyttäjätunnukset:

- **Järjestelmänvalvoja** (Administrator) on verkonvalvojan tunnus, jolla kaikki mahdolliset oikeudet toimialueella ja NT-työasemassa

- **Vieras** (Guest) on asennusvaiheessa luotu **Vieras** (Guest)-tunnus, jolla kuka tahansa pääsee ilman käyttäjätunnusta käyttämään NT-palvelimen jakamia resursseja. Termi tällaiselle kirjautumiselle on *Guest Logon* ja se tarvitaan eri verkkokäyttöjärjestelmien tukea varten. Oletuksena käyttäjätunnus (tili) on **poistettu käytöstä** (**Account Disabled**).

Seuraavat **paikalliset käyttäjäryhmät** ovat sekä NT-työasemassa että NT-palvelimessa (NT-työasemassa ei muita ryhmiä kuin paikallisia voi ollakaan):

- **Käyttäjät** (Users) - peruskäyttäjien **paikallinen** ryhmä. Ryhmällä on riittävät oikeudet operoida NT-työasemassa **loppukäyttäjänä**. Oikeuksiin ei kuulu esimerkiksi sivutustiedoston asettaminen jne, vaan seuraavan tyyppiset perusoperaatiot: sovellusten suorittaminen, tiedostojen hallinta, työaseman/palvelimen jakamien resurssien käyttäminen verkon kautta jne. Ryhmässä on mukana toimialueen **Domain Users** -ryhmä - myös NT-työasemassa, jos se on **liitetty toimialueeseen.** Oletuksena ryhmän jäsenet pääsevät kirjoittautumaan NT-työasemaan käyttäjäksi ja NT-työasemasta voi kirjautua toimialueelle, mutta NT-palvelimeen ei pääse käyttäjäksi esimerkiksi palvelimen näppäimistöstä!

- **Järjestelmänvalvojat** (Administrators) - tällä **paikallisella** ryhmällä on kaikki oikeudet halllita NT-työasemaa tai -toimialuetta: käyttäjätunnusten ja -ryhmien hallinta, resurssien hallinta, kiintolevyjen käsittelyt, ottaa omistukseen mikä tahansa objekti, varmistaa koko järjestelmä jne. Ryhmässä on mukana **paikallinen Järjestelmänvalvoja** (Administrator)-käyttäjätunnus sekä **toimialueen Domain Admins** -ryhmä. Domain Admins -ryhmä kuuluu mukaan paikalliseen **Järjestelmänvalvojat** (Administrators) -ryhmään myös NT-työasemassa, jos se on liitetty toimialueeseen

- **Vieraat** (Guests) - ryhmään kuuluu vain asennusvaiheessa luotu **Guest**-käyttäjätunnus, jolla kuka tahansa pääsee ilman käyttäjätunnusta käyttämään NT-palvelimen jakamia resursseja. Tällainen tarvitaan eri verkkokäyttöjärjestelmien tukea varten. Oletuksena tunnus on poistettu käytöstä (**Account Disabled**). NT-työasemassa ryhmässä on mukana **Vieras** (Guest)-käyttäjätunnus sekä toimialueella **Guests**-ryhmään kuuluu toimialueen yleinen **Domain Guests** -ryhmä. Jos **Guest**-käyttäjätunnus otetaan käyttöön (**Account Disabled** ei ole valittu), toimialueelle kirjautumaton käyttäjä pääsee esimerkiksi selaamaan toimialueen resursseja

- **Varmuuskopiointioperaatorit** (Backup Operators) ryhmän jäsenillä on oikeus varmistaa ja palauttaa mitä tahansa tiedostoja ohittaen tiedostojen suojaukset

- **Monistus** (Replicator) on tiedostojen monistukseen liittyvä ryhmä; ryhmän jäsenillä on oikeus viedä/tuoda tiedostoja

- **Tehokäyttäjät** (Power Users) tehokäyttäjien paikallinen ryhmä: peruskäyttäjien oikeuksien lisäksi kyseeseen tulevat hakemistojen ja kirjoittimien jakaminen, käyttäjätunnusten luominen ja itse luotujen käyttäjätunnusten hallinta sekä ajan asettaminen. Ryhmä on myös NT-palvelimessa, mutta **vain** jos palvelin on asennettu **Server**-tyyppisenä.

Seuraavat paikalliset ryhmät luodaan NT-palvelimeen, joka toimii toimialueen **ensisijaisen ohjauskoneena** (*Primary Domain Controller*, PDC):

- **Server Operators** - ryhmän oikeuksiin kuuluvat resurssien jakaminen, palvelimen lukitseminen, kirjautuminen palvelimel-

le jne

- **Print Operators** - ryhmän oikeuksiin kuuluu kirjoittimien hallinta

- **Account Operators** - käyttäjätunnusten ja -ryhmien hallinta; ei voi hallita kuitenkaan **Administrators**- tai **Server Operators** -ryhmiä

Seuraavat **yleiset ryhmät** luodaan NT-palvelimeen, joka toimii toimialueen **pääohjauskoneena** (*Primary Domain Controller*, PDC):

- **Domain Admins** - toimialueen pääkäyttäjät; on mukana **Administrators**-ryhmässä

- **Domain Users** - toimialueen peruskäyttäjät; on mukana **Users**-ryhmässä. Oletuksena **kaikki toimialueelle luotavat käyttäjät** kuuluvat tähän ryhmään

- **Domain Guests** - toimialueen vieraat; ryhmään kuuluu **Guest**-tunnus.

Huomattavaa:

- Vaikka käyttäjä (esimerkiksi tukihenkilö) kuuluisikin **kaikkiin** muihin ryhmiin paitsi **Järjestelmänvalvojiin** (Administrators), hän ei silti saavuta järjestelmänvalvojien oikeustasoa, koska käyttäjällä ei esimerkiksi ole oikeutta hallinnoida järjestelmänvalvojien käyttäjätunnuksia!

- Oletuskäyttäjätunnuksia **Järjestelmänvalvoja (Administrator)** ja **Vieras** (Guest) et voi poistaa, mutta voit disabloida tai uudelleennimetä ne!

- Jos **Vieras** (Guest)-tunnus on käytössä, niin **Kaikki** (Everyone)-ryhmälle jaetut resurssit ovat kenen tahansa (myös millekään toimialueelle kirjautumattoman) käyttäjän käytettävissä, koska Guest-tunnus kuuluu toki myös **Kaikki** (Everyone)-ryhmään

- Jos käyttäjän tunnusta ei ole määritelty toimialueella tai työasemassa, niin jaettuihin resursseihin saattaa päästä käsiksi

Guest Logonin avulla, jos **Vieras** (Guest)-tunnus ei ole pois käytöstä. Tavallisesti tällaista ei haluta, niinpä **Vieras** (Guest)-tunnuksen olisi myös hyvä pysyä disabloituna! Oletuksena käyttäjätunnus on disabloitu toimialueella, mutta ei NT-työasemassa. Voit myös käyttää sopivasti **Access This Computer From Network**- ja **Log On Locally** -oikeuksia rajoittaaksesi **Vieras** (Guest)-tunnuksen käyttöä. Katso myös **luku 11**.

- Tee kopioita **Administrator**-käyttäjätunnuksesta - yksi tai useampia.Tähän on kaksi syytä:

  - Jos Administrator-käyttäjätunnus lukitaan (Account Locked Out) tai sen salasana unohtuu, NT pitää pahimmassa tapauksessa asentaa uudelleen. Erityisen harmillista tämä on toimialueen tapauksessa

  - Jos useampi **Administrator** puuhailee samaan aikaan verkossa, on hankala selvittää kuka itseasiassa teki tai tekee mitäkin. Luomalla esimerkiksi käyttäjälle JKI **käyttäjäkohtainen** Administrator-tunnus (vaikkapa ADMIN_JKI) saadaan tilanteeseen selvyyttä. Alkuperäisen Administrator-käyttäjätunnuksen salasana pidetään visusti tallessa.

  - Administrator-käyttäjätunnuksen voi uudelleenimetä tai disabloida, mutta sitä ei voi poistaa!

  - Administrator-käyttäjätunnuksen pystyy *ehkä* palauttamaan **korjauslevykkeeltä** (*Emergency Repair Disk*).

Yleiset ja paikalliset ryhmät

Riippuen siitä, onko kyseessä Windows NT -työaseman käyttäjätietokanta vai toimialueen ensisijaisen ohjauskoneen (Primary Domain Controller, PDC) käyttäjätietokanta, käyttäjätietokannassa voi esiintyä kahdenlaisia ryhmiä.

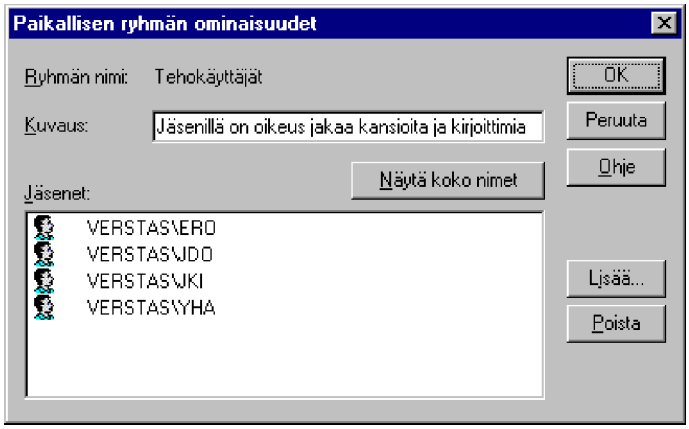
Paikallinen ryhmä (Local Group) on ryhmä, johon voi kuulua **paikallisia käyttäjiä** ja **yleisiä ryhmiä** (Global Group), mutta ei toisia paikallisia ryhmiä.

NT-työaseman **Käyttäjien hallinta** (User Manager) ei ymmärrä eikä pysty luomaan muita kuin **kyseisen NT-työaseman paikallisia ryhmiä**; tällöin ryhmät ja käyttäjät ovat käsiteltävissä ja käytettävissä vain NT-työasemassa paikallisesti.

Jos työasema on liittynyt toimialueeseen, **Käyttäjien hallinnalla** (User Manager) voidaan lisätä työaseman paikallisiin ryhmiin kuitenkin myös **toimialueen yleisiä ryhmiä** ja **yleisiä käyttäjiä**, mutta niitä ei voida luoda eikä muokata. Myöskään **toimialueen paikallisia käyttäjiä** tai **paikallisia ryhmiä** ei voida lisätä työaseman käyttäjäryhmiin tai käyttäjiksi.

Paikallisia ryhmiä työasemassa ovat mm. **Käyttäjät** (Users) peruskäyttäjille, **Tehokäyttäjät** (Power Users) tehokäyttäjille ja **Järjestelmänvalvojat** (Administrators) työaseman valvojille hallintakäyttöä varten.

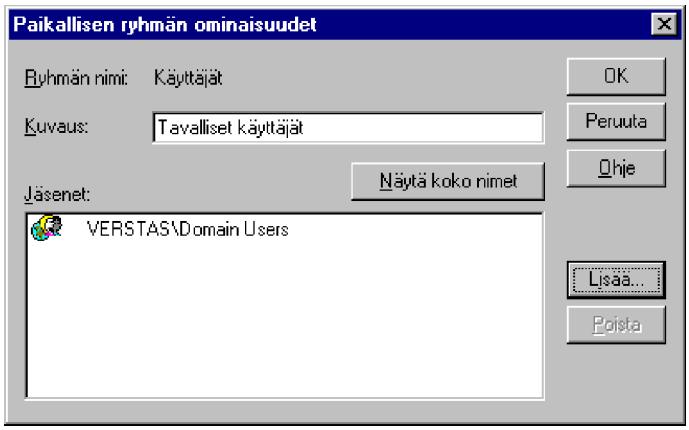
Käyttäjien hallinta (User Manager) näyttää tässä työasemassa paikallisen ryhmän **Tehokäyttäjät** (Power Users) jäseniksi vain toimialueen yleisiä käyttäjätunnuksia:



Käyttäjäryhmät, jotka alkavat etuliitteellä **Toimialueen...** (Domain) ovat **aina** toimialueella määriteltyjä käyttäjäryhmiä.

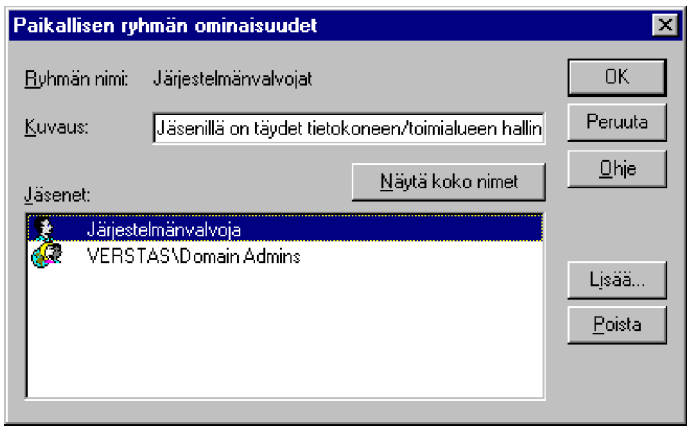
Toimialueen yleinen käyttäjien ryhmä **Domain Users** lisätään automaattisesti työaseman paikalliseen **Käyttäjät** (Users)-ryhmään, kun työasema lisätään toimialueelle; tällöin työaseman paikalliseen käyttäjäryhmään kuuluvat automaattisesti myös kaikki toimialueen käyttäjätunnukset.

Koska tässä esimerkin tapauksessa jälleen työaseman versio on suomenkielinen Windows NT 4.0 Workstation, ja toimialueen PDC on englanninkielinen Windows NT 4.0 Server, niin myös ryhmän nimi on **Domain Users**:



Vastaavasti toimialueen yleinen järjestelmänvalvojien ryhmä **Domain Admins** lisätään automaattisesti työaseman paikalliseen **Järjestelmänvalvojat** (Administrators)-ryhmään, kun työasema lisätään toimialueelle.

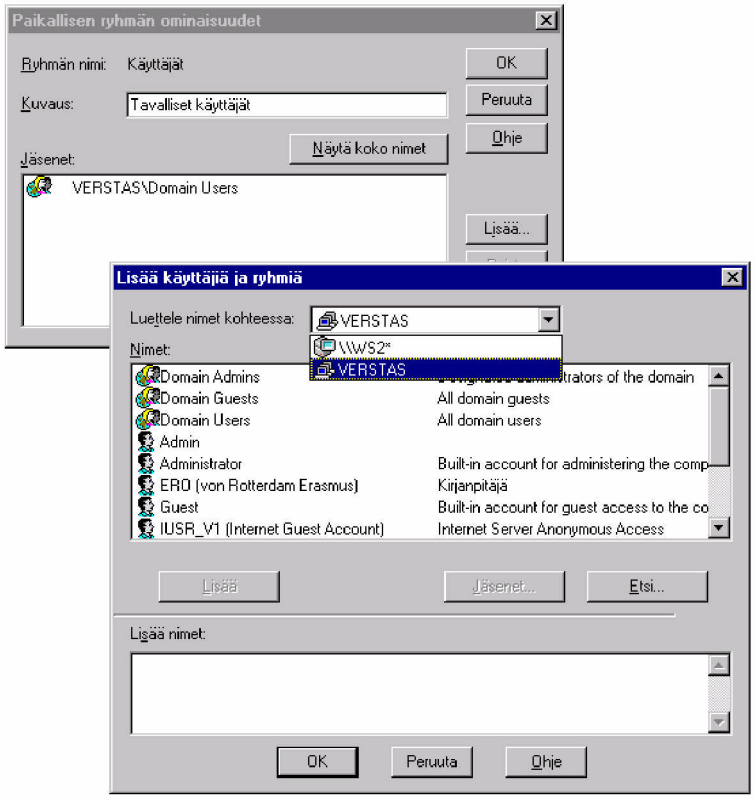
Tällöin työaseman paikalliseen järjestelmänvalvojien ryhmään kuuluvat automaattisesti myös kaikki toimialueen järjestelmänvalvojien käyttäjätunnukset. Oletuksena ryhmään kuuluu joka tapauksessa myös **työaseman paikallinen Järjestelmänvalvoja** (Administrator)-käyttäjätunnus.



Edellä mainitut ryhmäjäsenyydet helpottavat hallintaa huomattavasti, koska nyt riittää käyttäjätunnuksien määrittely vain toimialueella! Jos työasema on liitetty toimialueelle, tämä ryhmien lisääminen on siis jo tehty automaattisesti.

Toimialueelle liitetyssä NT-työasemassa voit valita, lisätäänkö käyttäjiä paikalliseen ryhmään työaseman käyttäjätietokannasta (WS2) vai toimialueelta (VERSTAS). Jos toimialueelta on luottosuhteita toisiin toimialueisiin, niidenkin nimet näkyisivät luettelossa, ja näiden toimialueiden

yleiset käyttäjätunnukset ja yleiset käyttäjäryhmät olisivat siis lisättävissä johonkin NT-työaseman paikalliseen ryhmään.
User Manager for Domains sen sijaan hallitsee paitsi paikalliset, myös

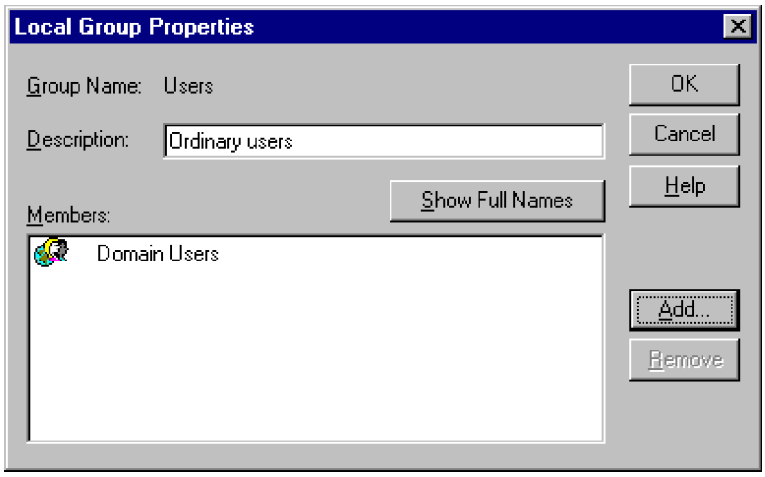


yleiset ryhmät (Global Groups) ja yleiset käyttäjätunnukset. Yleinen ryhmä ja yleinen käyttäjä näkyvät toimialueeseen kuuluvassa NT-työasemassa ja luottosuhteen yli toisessakin toimialueessa; **toimialueen paikallinen käyttäjä** tai **paikallinen ryhmä** ei näy, eikä sitä voida lisätä toisen toimialueen käyttäjäryhmiin.

Toimialueen paikallisia ryhmiä ovat mm. **Users** peruskäyttäjille ja **Administrators** valvojille toimialueen paikallista hallintakäyttöä varten.

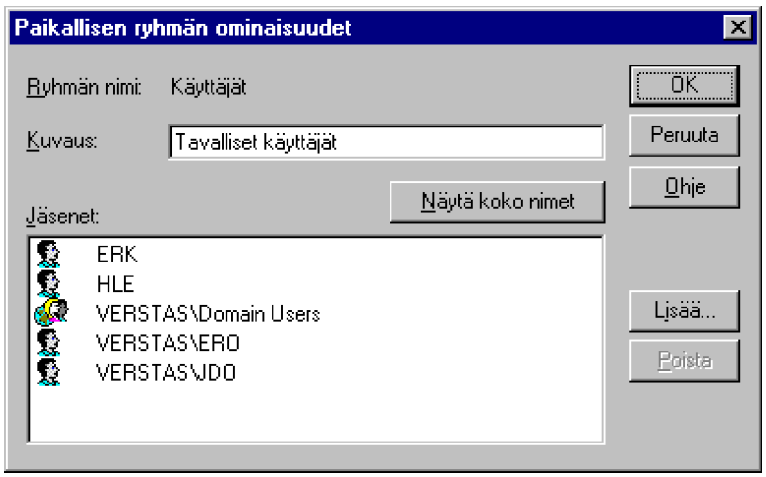
Toimialueen yleisiä ryhmiä ovat mm. **Domain Users** peruskäyttäjille ja **Domain Admins** valvojille hallintakäyttöä varten.

Toimialueella yleinen ryhmä **Domain Admins** kuuluu mukaan toimialueen paikalliseen ryhmään **Administrators** ja yleinen ryhmä **Domain Users** kuuluu mukaan toimialueen paikalliseen ryhmään **Users**:

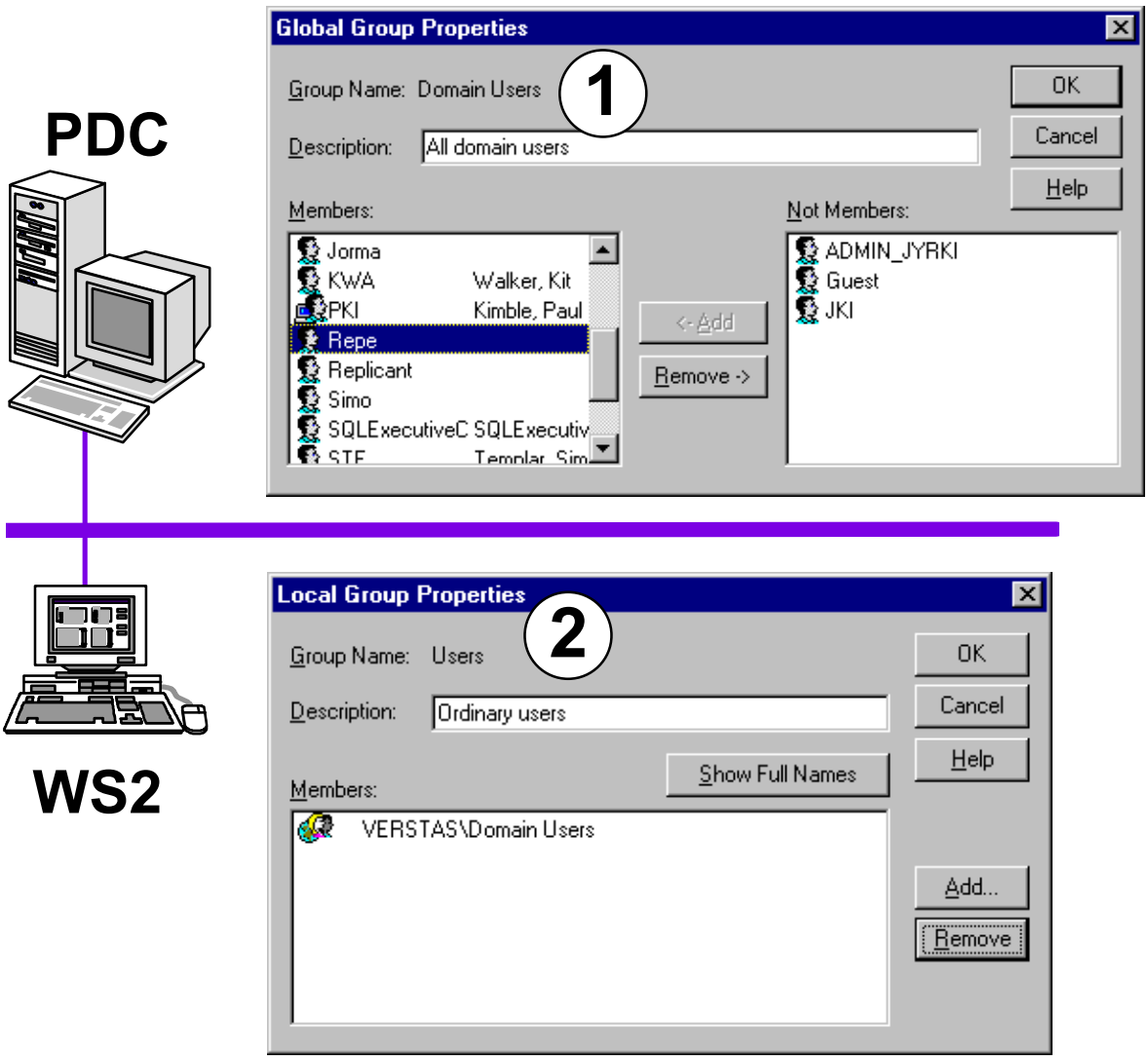


Kannattaa erityisesti muistaa se, että NT-työasemien ja toimialueen paikallisilla ryhmillä ei ole mitään tekemistä keskenään!

Tässä tarkastellaan **WS2**-työaseman paikallisen **Käyttäjät**-nimisen ryhmän jäseniä. Mukana on **kyseisessä työasemassa** määritellyt käyttäjätunnukset **ERK** ja **HLE** sekä **VERSTAS-nimisen toimialueen** käyttäjätunnukset **ERO** ja **JDO** ja **VERSTAS-toimialueen Domain Users**-käyttäjäryhmä.



Tässä esimerkissä **Domain Users-ryhmän** käyttäjä **Repe** saa **Domain Users-ryhmän** käyttöoikeudet kirjautuessaan toimialueelle **VERSTAS** (**1**).

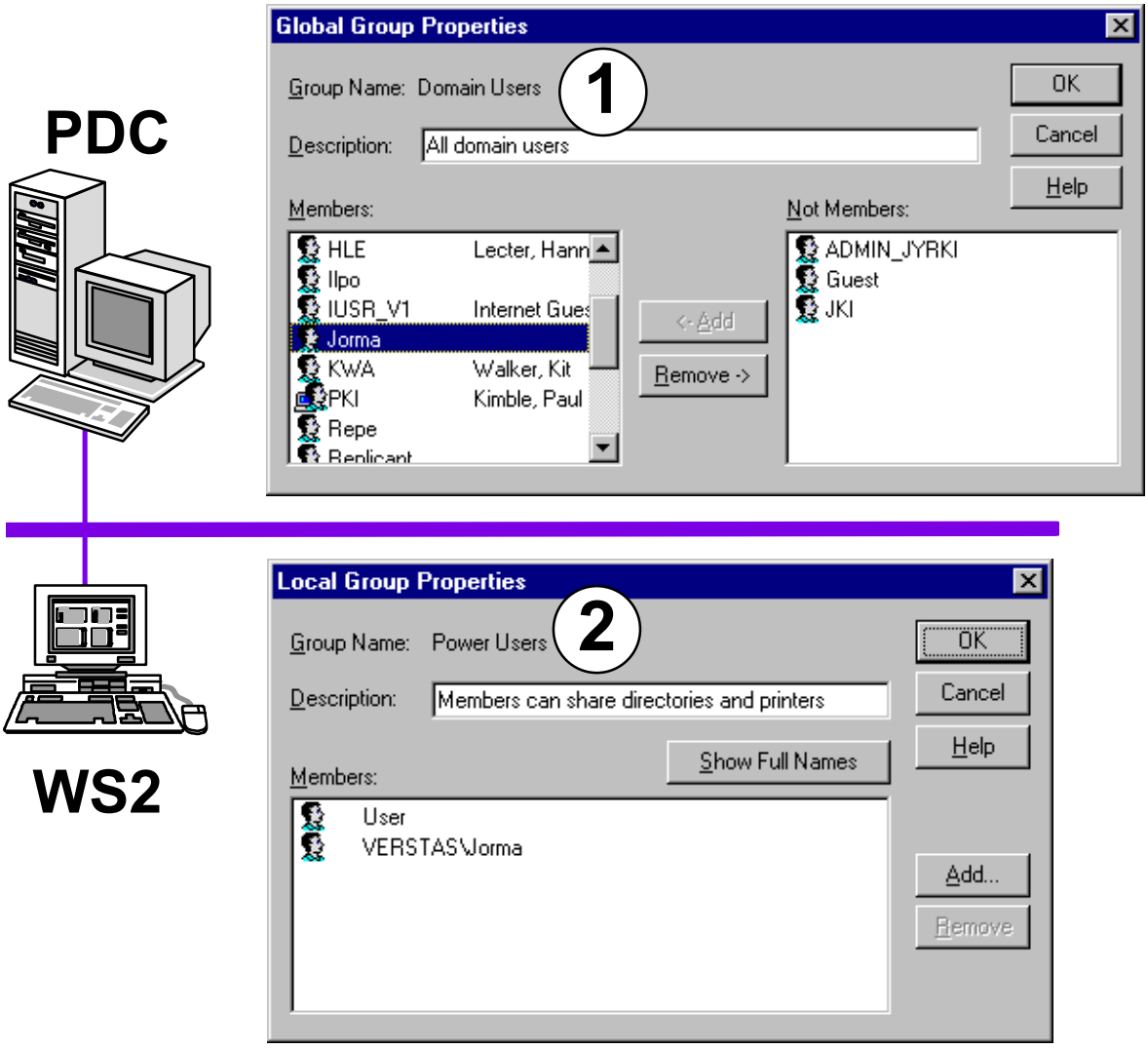


Työasemassa (**WS2**) hänellä on **Käyttäjien** (Users) oikeudet hallita työasemaansa (**2**), koska **VERSTAS**-toimialueen yleinen käyttäjäryhmä **Users** (=**VERSTAS\Users**) kuuluu työasemassa **WS2** paikalliseen **Käyttäjien** (Users) ryhmään. Työaseman paikalliseen **Käyttäjien** (Users) ryhmään ei kuulu esimerkiksi ollenkaan työasemassa paikallisesti määriteltyjä käyttäjätunnuksia. Niitä ei itse asiassa tarvita ollenkaan, jos käyttäjätunnusten hallinta halutaan keskittää toimialueelle.

Peruskäyttäjän oikeuksilla (=työaseman **Käyttäjien** (Users) ryhmä) ei voi esimerkiksi muuttaa työaseman kellonaikaa / päiväystä tai Ohjauspaneelin järjestelmätason asetuksia.

Mahdollisuus lisätä toimialueen yleisiä käyttäjiä NT-työaseman paikallisiin ryhmiin mahdollistaa kuitenkin sen, että voit lisätä halutun toimialueen käyttäjän yksittäisessä NT-työasemassa esimerkiksi paikalliseen **Tehokäyttäjien** (Power Users)-ryhmään.

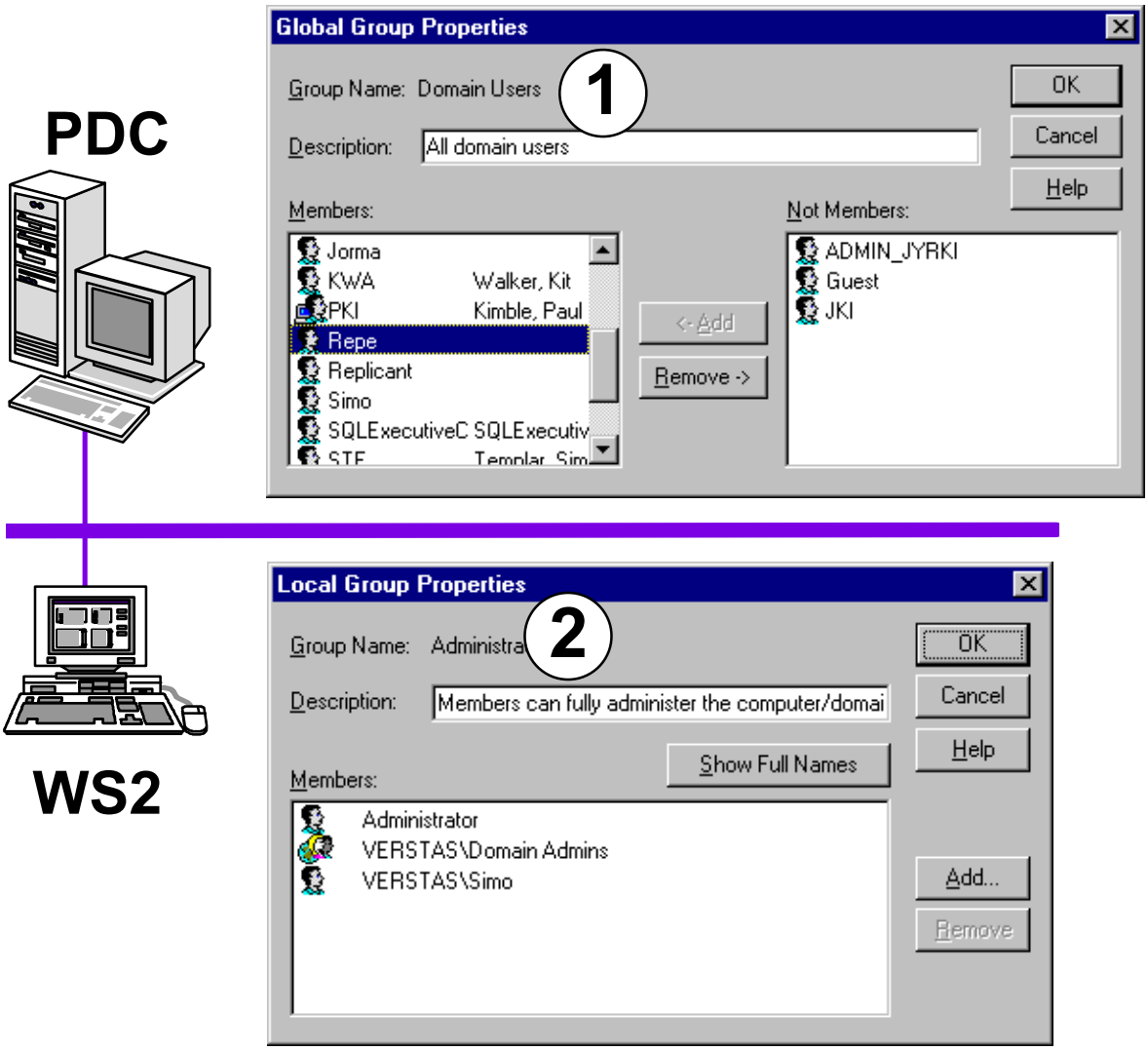
Tällöin käyttäjä kirjautuessaan toimialueelle toimialueella määritellyllä käyttäjätunnuksellaan saa toimialueen ryhmäjäsenyyksistä riippuen esimerkiksi vain **Domain Users-ryhmän** käyttöoikeudet toimialueen palvelimiin (ja NT-työasemiin), mutta omassa työasemassaan hänellä on **Tehokäyttäjien** (Power Users) oikeudet hallita työasemaansa (jakaa hakemistoja, kirjoittimia jne).



Tässä esimerkissä **Domain Users-ryhmän** käyttäjä **Jorma** saa **Domain Users-ryhmän** käyttöoikeudet kirjautuessaan toimialueelle **VERSTAS** (**1**), mutta omassa työasemassaan (**WS2**) hänellä on **Tehokäyttäjien** (Power Users) oikeudet hallita työasemaansa (**2**), koska VERSTAS-toimialueen käyttäjä Jorma (=**VERSTAS\Jorma**) kuuluu työasemassa **WS2** paikalliseen **Tehokäyttäjien** (Power Users) ryhmään.

Niissä työasemissa, joissa tällaista liitosta ei ole tehty, käyttäjän käyttöoikeudet työasemassa todennäköisesti ovat vain työaseman paikallisen **Käyttäjät (Users)-ryhmän** oikeudet, koska toimialueen **Domain Users-ryhmä** kuuluu oletuksena toimialueen NT-työasemien paikalliseen **Käyttäjät (Users)-ryhmään** mukaan! Liitos tehdään kun NT-työasema liitetään toimialueelle. Muut ryhmäjäsenyydet on aina erikseen luotava.

Jos **Tehokäyttäjien** (Power Users)-ryhmän oikeudet eivät käyttäjälle riitä, toimialueen käyttäjätunnus voidaan lisätä työaseman paikalliseen **Järjestelmänvalvojien** (Administrators)-ryhmään. Tällöin käyttäjä kirjautuessaan toimialueelle toimialueella määritellyllä käyttäjätunnuksellaan saa vain **Domain Users-ryhmän** käyttöoikeudet toimialueen palvelimiin, mutta omassa työasemassaan hänellä on **Järjestelmänvalvojien** (Administrators) oikeudet hallita työasemaansa. Muissa toimialueen työasemissa ja palvelimissa käyttäjällä on edelleen **Domain Users-ryhmän** käyttöoikeudet.



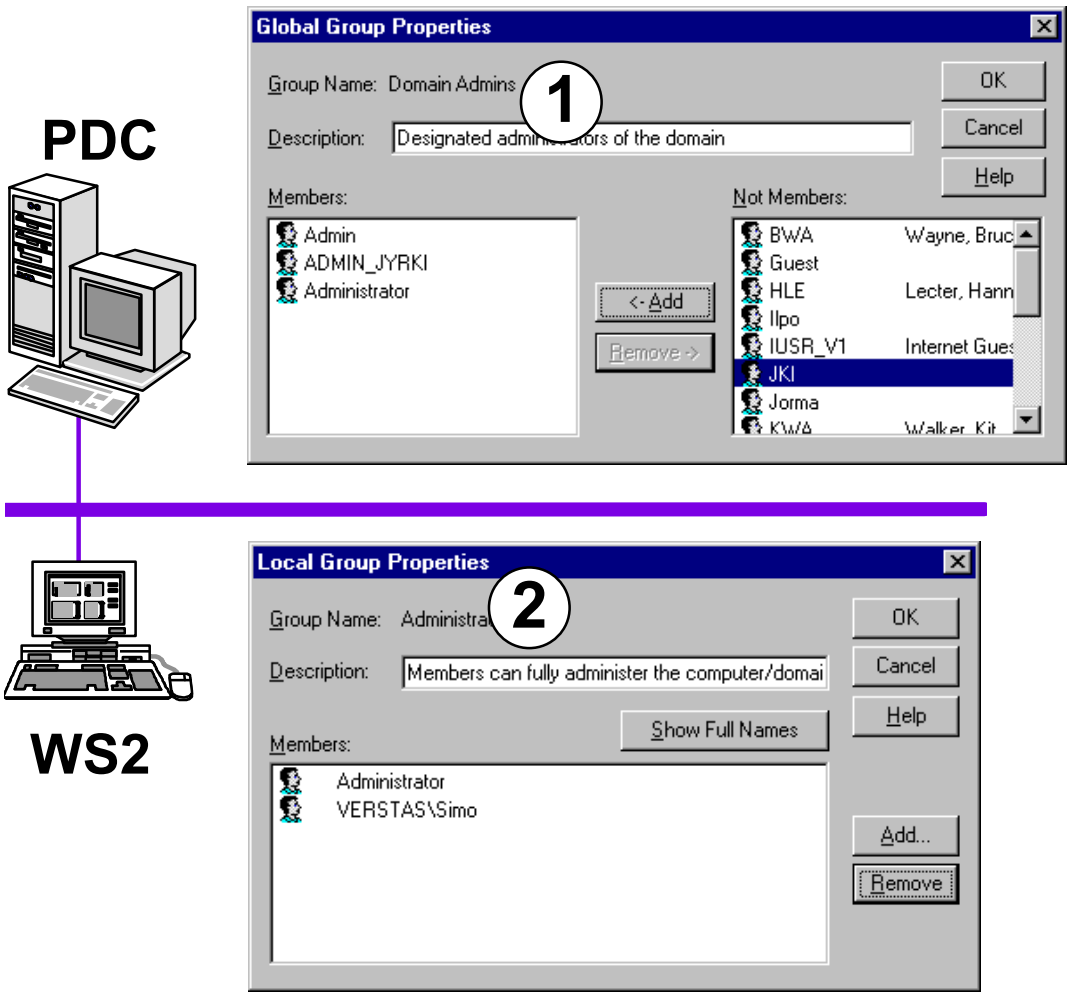
Tässä esimerkissä **Domain Users-ryhmän** käyttäjä **Simo** saa **Domain Users-ryhmän** käyttöoikeudet kirjautuessaan toimialueelle **VERSTAS** (**1**), mutta työasemassa (**WS2**) hänellä on **Järjestelmänvalvojien** (Administrators) oikeudet hallita työasemaa (**2**), koska VERSTAS-toimialueen käyttäjä **Simo** (=**VERSTAS\Simo**) kuuluu työasemassa **WS2** paikalliseen **Järjestelmänvalvojien** (Administrators) ryhmään.

Sama periaate toimii **luottosuhteiden** avulla toimialueiden välillä.

NT-työaseman hallintaoikeuksia voidaan myös **rajoittaa**.

Tässä esimerkissä kirjautuessaan toimialueelle käyttäjä **Simo** ei taatusti kuulu toimialueella **Domain Admins**-ryhmään (**1**), mutta työasemassa **WS2** hänellä on **Järjestelmänvalvojien** (Administrators) oikeudet hallita työasemaa. Muissa toimialueen työasemissa ja palvelimissa käyttäjällä on ehkäpä edelleen **Domain Users-ryhmän** käyttöoikeudet.

Huomaa, että **Domain Admins**-ryhmä **on poistettu työaseman WS2 paikallisesta Järjestelmänvalvojien** (Administrators) ryhmästä! Poistaminen edellyttää **Järjestelmänvalvojien** (Administrators) oikeuksia a.o. työasemassa, jotea aivan vahingossa tällaista ei voi tapahtua, mutta tämäkin on mahdollista.

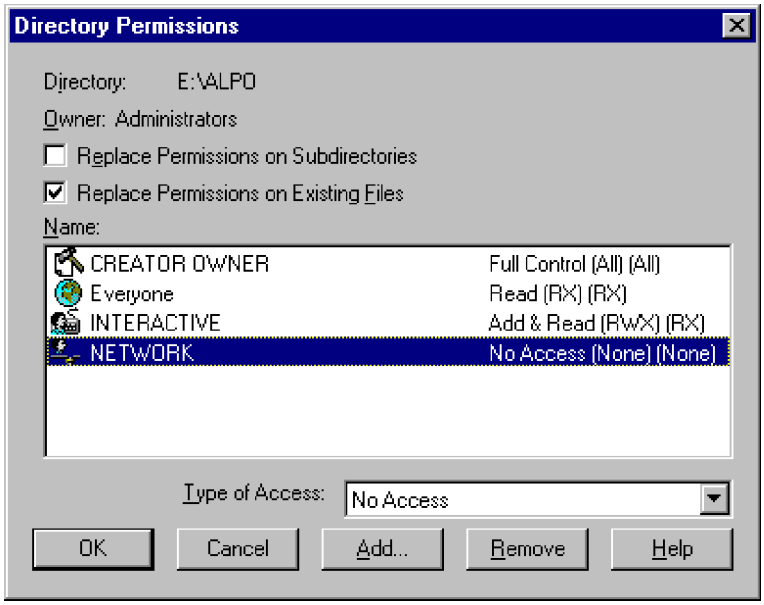


Käyttäjätunnusten ja ryhmien lisäksi voit määritellä käyttäjien oikeuksia (User Rights) tarpeen mukaan. Voit esimerkiksi rajoittaa **Kirjautuminen paikallisesti** (Log on locally) oikeuksia.

Erikoiskäyttäjätunnukset ja -ryhmät

NT:ssä on myös **erikoisryhmiä**, joita et kuitenkaan näe **Käyttäjien hallinnassa** (User Manager). Näitä ryhmiä et voi uudelleennimetä etkä poistaa:

- **Verkko (Network)** - kuka tahansa käyttäjä, joka käyttää jaettua resurssia verkon kautta
- **Vuorovaikutteinen (Interactive)** - käyttäjä, joka on kirjautunut paikallisesti käyttäjäksi ja käyttää paikallisia resursseja
- **Kaikki (Everyone)** - kaikkien toimialueiden kaikki käyttäjät, vieraat jne. Tälle ryhmälle on annettu oletuksena kaikki oikeudet jaettaessa resursseja
- **Luoja-omistaja (Creator Owner)** - ryhmä sisältää käyttäjän, joka loi objektin (tiedoston, tulostustyön jne). Voit esimerkiksi määritellä NTFS-osiolla **Kaikki** (Everyone)-ryhmälle vain **luku-oikeudet** (Read), mutta **Luoja-omistajalle** (Creator Owner) **täydet oikeudet** (Full Control).



Toimialueet

Windows NT -työaseman käyttäjäasetukset ja -oikeudet perustuvat **työryhmämalliin**, eli resurssit jaetaan ja suojataan työasemakohtaisesti - eri tasoiset käyttöoikeudet voidaan erotella paikallisesti työasemassa määriteltyjen käyttäjätunnusten avulla. Tämä on ns. *User Level Security*, mikä edellyttää käyttäjätunnusten luomista ja resurssien eritasoisten käyttöoikeuksien jakamista käyttäjäkohtaisesti.

Haluttaessa keskitetty käyttäjien ja resurssien hallinta pitää tukeutua Windows NT -palvelimiin. Tällöin voidaan hyödyntää toimialueen (*domain*) keskitetyn resurssienhallinnan etuja.

Jos yksi toimialue ei riitä tai ei ole mahdollinen, niin joudutaan miettimään **luottosuhteita** (*Trust Relationship*) ja eri **toimialuemalleja**.

Useita eri toimialueita voidaan tarvita eri syistä:

- Organisatoriset syyt (kustannuspaikat, paikallinen tuki, toiminnan erilaisuus eri yksiköissä)
- Maantieteelliset syyt (etäisyydet resurssien ja käyttäjien välillä)
- Ongelmalliset linjayhteydet
- Tietoturvasta ja esimerkiksi Internet-yhteyksistä johdetut syyt.

Jos kuitenkin halutaan keskitetty käyttäjien hallinta tai jos halutaan, että eri toimialueiden käyttäjät voivat käyttää yhteisiä resursseja, joudutaan miettimään lisäksi käyttäjien hallintaa toimialueiden välillä.

Palvelinten roolit

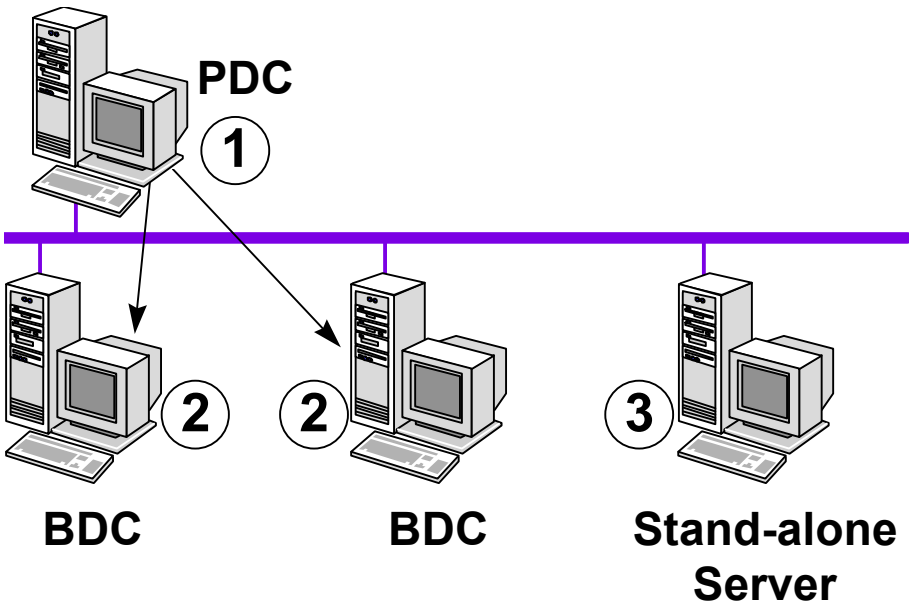
Asennettaessa NT-palvelin tulee ottaa kantaa siihen, mikä on palvelimen rooli verkossa. Näitä rooleja voi olla kolme:

1) **Ensisijainen** ohjauskone (*Primary Domain Controller*, PDC) (kuvassa **(1)**) asennetaan aina toimialueen ensimmäisenä palvelimena, mutta myöhemmin jokin muu ohjauskone (BDC) voidaan

ylentää pysyvästi tai väliaikaisesti PDC:ksi esimerkiksi huollon ajaksi. PDC ylläpitää käyttäjätietokantaa ja toimialueen asetuksia sekä käsittelee käyttäjän kirjautumispyynnöt toimialueelle. Lukumäärä on rajoitettu toimialueittain: voi olla vain yksi PDC toimialuetta kohti. Myös PDC voi toimia tiedosto-, tulostin- tai sovelluspalvelimena, mutta käyttäjämääriltään suurissa verkoissa PDC ei tee muuta kuin ylläpitää keskitettyä käyttäjätietokantaa ja sen päivityksiä.

2) **Ohjauskone** eli varapalvelin tai varakone (*Backup Domain Controller*, BDC) saa kopion PDC:n käyttäjätietokannasta (kuvassa **(2)**). Samalla se toimii PDC:n varapalvelimena, jos PDC ei ole jostain syystä verkossa, koska varapalvelin käsittelee myös käyttäjän kirjautumispyynnöt toimialueelle. Toimialue ei edellytä yhtään varapalvelinta, mutta suositukseni on vähintään yksi kappale toimialuetta kohti; maksimilukumäärää ei ole rajoitettu. BDC voi toimia tiedosto-, tulostin- tai sovelluspalvelimena

3) **Palvelin** (Server tai Stand-Alone Server) (kuvassa **(3)**) voi toimia tiedosto-, tulostin- tai sovelluspalvelimena. Palvelin ei kuitenkaan saa kopiota PDC:n käyttäjätietokannasta, mikä edellyttää käyttäjien hallintaa paikallisesti palvelimessa.



Saman toimialueen sisällä toimialueeseen kuuluvien palvelimien (erityisesti ohjauskoneiden, *Domain Controllerien*) välillä on oltava pysyvä yhetys. Tavallisesti kyseeseen tulee vähintään 64 kbps kiinteä linja. Siksi

RAS-yhteys ei tule kyseeseen saman toimialueen eri palvelimien välille.

Primary Domain Controller

Palvelinten rooleja on käsitelty jo asennuksen yhteydessä, mutta palvelimen roolilla on keskeinen merkitys siinä, miten sen käyttäjätietokantaa käsitellään.

Ensisijainen ohjauskone (Primary Domain Controller, PDC):

- Asennetaan toimialueen ensimmäisenä palvelimena
- Ylläpitää käyttäjätietokantaa ja toimialueen asetuksia
- Käsittelee käyttäjän kirjautumispyynnöt toimialueelle **Net Logon**-palvelun avulla
- Voi toimia tiedosto-, tulostin- tai sovelluspalvelimena
- Lukumäärä on **tasan yksi kappale per toimialue**

Minkä tahansa saman toimialueen BDC:n voi ylentää (*Promote*) **Server Manager**-ohjelmalla PDC:ksi. Muutoksen eri vaiheet tehdään tällöin automaattisesti. Roolin muutos kestää joitakin minuutteja - riippuen käyttäjätietokannan koosta sekä verkon nopeudesta. Laajassa verkossa (jossa on useita satoja tai tuhansia käyttäjiä) roolin muutokseen saattaa mennä enemmänkin aikaa, mutta toisaalta laajoissa verkoissa on käytettävissä tällä välin *yleensä* myös jokin toinen BDC, joka hoitaa operaation aikana käyttäjien verkkoonkirjautumiset.

Muistettavaa:

- Jos PDC ei ole käytettävissä (esimerkiksi kaatunut tai ei ole verkossa), niin käyttäjätietokannan muuttaminen ei onnistu, ei esimerkiksi myöskään käyttäjien oikeusmääritysten, (*User Rights*) tai salasanojen asetusten muuttaminen.
- Jos PDC on täysin hajonnut, voit ylentää jonkin BDC:n pysyvästi PDC:ksi, mutta muista että et tuo tämän jälkeen alkuperäistä PDC:tä verkkoon!

PDC ei ole siirrettävissä toiseen toimialueeseen ilman uudelleenasennusta. **Vasta Windows NT 5.0 tuo tähän tervetulleen muutoksen**.

Backup Domain Controller

Ohjauskone (Backup Domain Controller, BDC) (myös nimityksiä varakone tai varapalvelin käytetään):

- Saa automaattisesti kopion PDC:n käyttäjätietokannasta sekä käyttäjätietokannan päivitykset
- Toimii varapalvelimena, jos ensisijainen ohjauskone (PDC) ei ole jostain syystä verkossa ja voi tällöin hoitaa käyttäjien verkkoon kirjautumispyynnöt **Net Logon**-palvelun avulla. Koska BDC käsittelee käyttäjän kirjautumispyynnöt toimialueelle, se siten myös tasaa PDC:n kuormitusta. Käyttäjän kirjautumisessa se vertaa omaa kopiotaan toimialueen keskitetystä käyttäjätietokannasta, ja sen mukaan hyväksyy tai hylkää käyttäjän kirjautumispyynnön
- Voi toimia tiedosto-, tulostin- tai sovelluspalvelimena
- Toimialue ei edellytä yhtään varapalvelinta, mutta oma suositukseni **on vähintään yksi kappale per toimialue**; maksimi lukumäärää ei ole rajoitettu
- Jos BDC ei jaa resurssejaan verkkoon, jopa **i486/33** riittävällä muistilla (32 Mt tai enemmän) *saattaa* riittää; tilannetta voit valvoa **Performance Monitorilla**.

Käyttäjätietokannan voit synkronoida **Server Manager**-ohjelmalla - joko siten, että PDC lähettää päivitykset kaikille BDC:eille tai valittu BDC lähettä päivityspyynnön PDC:lle.

Muistettavaa:

- Ilman toimivaa vähintään yhtä ohjauskonetta (*Domain Controller*) käyttäjät eivät voi kirjautua toimialueelle!
- Jos PDC ei ole käytettävissä, käyttäjätietokannan muuttaminen ei onnistu.

BDC ei ole siirrettävissä toiseen toimialueeseen ilman uudelleenasennusta. Windows NT 5.0 tuo tähän muutoksen.

Stand-Alone Server

Palvelin (Stand-Alone Server tai Server, myös termiä **Member Server** käytetään):

- Voi toimia tiedosto-, tulostin- tai sovelluspalvelimena
- Ei saa kopiota käyttäjätietokannasta - edellyttää siis omaa **paikallista** käyttäjien hallintaa User Manager for Domains-ohjelmalla.

Stand-Alone Server-tyyppisen palvelimen liittäminen toimialueelle voidaan tehdä asennuksen yhteydessä tai jättää palvelin liittyneeksi työryhmään:

- **Palvelin liitetty työryhmään** (Workgroup) - Stand-Alone Server-tyyppinen palvelin toimii kuten työryhmään määritelty NT-työasema. Ei minkäänlaista keskitettyä käyttäjien hallintaa - käyttäjät määritellään työasemakohtaisesti palvelimen käyttäjien hallinnalla. Ei myöskään keskitettyä resurssien käyttöoikeuksien hallintaa
- **Palvelin liitetty toimialueelle** (Domain) - Stand-Alone Server-tyyppinen palvelin toimii kuten NT-työasema. Voidaan tukeutua toimialueen keskitettyyn käyttäjien hallintaan - esimerkiksi käyttäjien ryhmäjäsenyydet voidaan määritellä (kuten palvelimen paikalliseen **Users**-ryhmään voidaan lisätä toimialueen **Domain Users**-ryhmä mukaan). Resurssien käyttöoikeuksien hallinta voidaan toteuttaa käyttämällä hyväksi toimialueen yleisiä käyttäjätunnuksia ja -ryhmiä. Resurssien hallinta voidaan hoitaa esimerkiksi NT-palvelimelta tai toisesta toimialueelle liittyneestä NT-työasemasta.

Stand-Alone Server on siirrettävissä toiseen toimialueeseen tai työryhmään, mutta siinäkin se toimii Stand-Alone Server -tyyppisenä palvelimena.

Stand-Alone Server on sopiva ratkaisu joihinkin palvelintoimintoihin, mutta yhdenkin Stand-Alone Serverin ylläpito saattaa pahimmillaan aiheuttaa kaksinkertaisen määrän työtä!

Luottosuhteet

Luottosuhteilla (*Trust Relationship*) mahdollistetaan käyttäjien käyttöoikeuksien ulottaminen myös toisiin toimialueisiin; tällöin toisissa toimialueissa ei tarvitse määritellä uudelleen kyseistä käyttäjää, vaan luottosuhteen avulla käyttäjälle tai ryhmään, johon käyttäjä kuuluu, voidaan suoraan antaa halutut käyttöoikeudet. Samoin käyttäjä voi kirjautua yhdestä toimialueesta toisen toimialueen käyttäjäksi.

Luottosuhteita määritellään **User Manager for Domainsilla**. Niiden toimintaa voi valvoa Windows NT Resource Kitin **Domain Monitor**-apuohjelmalla.

Luottosuhteita ei voi määritellä Windows NT -työaseman käyttäjätietokannalla eikä työaseman **Käyttäjien hallinnalla** (User Manager), mutta työaseman käyttäjä voi kirjautua työaseman käyttäjäksi luotetun toimialueen käyttäjätunnuksella.

Luottosuhteeseen liittyy kaksi käsitettä; **luottava** (Trusting) ja **luotettu** (Trusted) toimialue. Tämä tarkoittaa sitä, että luottava toimialue luottaa toisen toimialueen käyttäjiin ja antaa heille käyttöoikeudet omalla toimialueellaan. Jos esimerkiksi toimialue **NNN** luottaa toimialueeseen **YYY**, niin tällöin toimialueen **YYY** käyttäjät ja käyttöoikeudet saadaan voimaan myös toimialue **NNN**:ssä.

Luottosuhde voi olla myös **kaksisuuntainen** (*Two-way trust*); molemmat toimialueet voivat luottaa toisiinsa. Luottosuhde ei ole kuitenkaan läpinäkyvä eli toimialueen läpi se ei voi ulottua. Luottosuhde pitää aina erikseen perustaa sekä luottavassa että luotetussa toimialueessa.

Luottosuhteilla mahdollistetaan käyttäjien käyttöoikeuksien ulottaminen myös toisiin toimialueisiin; tällöin toisissa toimialueissa ei tarvitse määritellä uudelleen kyseistä käyttäjää. Jos käyttäjä olisi määritelty useassa toimialueessa, esimerkiksi salasanan muutokset pitäisi kaikissa määritellä samanaikaisesti!

LAN Manager 2.x-versio ei tue luottosuhteita. Tällöin LAN Manager-palvelimia pitää käyttää NT:n *Single Domain*-toimialuemallissa.

Toimialuemallit

Luottosuhteilla (*Trust Relationships*) saadaan aikaan neljä erityyppistä toimialuemallia (*domain model*).

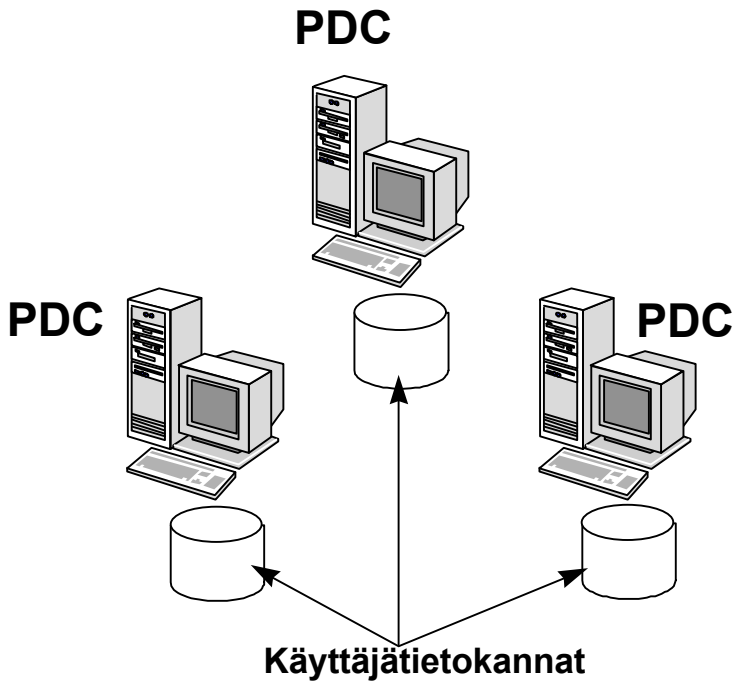
- Single domain
- Master domain
- Multiple master domain
- Complete Trust.

Näitä eri toimialuemalleja käsitellään seuraavaksi.

Single domain

Single domain -mallissa ei luoda minkäänlaisia luottosuhteita toimialueiden välille. Tällöin jokainen käyttäjä on määriteltävä jokaiseen toimialueeseen erikseen. Jos halutaan käyttää toisen toimialueen resursseja, se tapahtuu **Vieras** (Guest)-käyttäjätunnuksen oikeuksin tai luomalla tarvittava a.o. käyttäjätunnus paikallisena käyttäjänä molempiin toimialueisiin. Tästä taas seuraa salasanojen päivitysongelmat jne.

Tämä on ainoa LAN Managerin ymmärtämä toimialuemalli. LAN Manager-palvelinten tulee olla Windows NT -toimialueilla Member- tai Backup Server-tyyppisiä palvelimia.



Tässä esimerkissä on kolme toimialuetta (ja kolme ensisijaista ohjauskonetta, *Primary Domain Controlleria*).

Myös termiä *yksittäisten toimialueiden malli* jotkut yrittävät juurruttaa suomalaiseen ATK-sanastoon.

Master domain

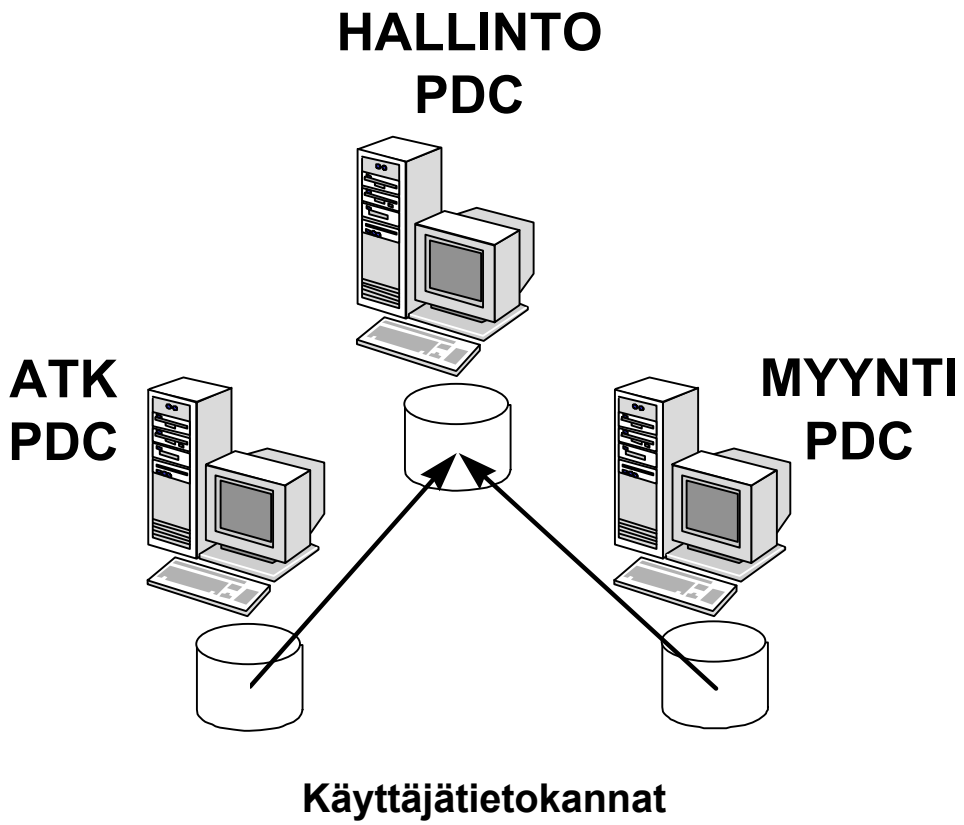
Master domain -mallissa on yksi toimialue, johon kaikki muut toimialueet luottavat - muut toimialueet eivät luota mihinkään muuhun toimialueeseen. Tällöin käyttäjät voidaan luoda keskitetysti vain yhdessä toimialueessa.

Malli sopii hyvin laajoihin verkkoihin (10 000 käyttäjää), joissa halutaan keskittää käyttäjätunnusten ylläpito. Toisaalta se tarjoaa myös mahdollisuuden hallita paikallisella pääkäyttäjätason (*Administrator*) tunnuksella verkkoa. Lisäksi Master Domainissa voidaan antaa yksittäiselle käyttäjälle eri oikeuksia eri toimialueissa. Esimerkiksi **Domain Users** -ryhmään käyttäjä voi kuitenkin kuulua yksittäisessä luottavassa toimialueessa

kyseisen toimialueen paikalliseen **Administrators**-ryhmään - samaan ryhmään, jossa jo on kyseisen toimialueen paikallinen **Administrator**-käyttäjätunnus.

Jos luottavat toimialueet ovat hitaan tietoliikenneyhteyden päässä, yksi luotetun toimialueen *Backup Domain Controller* kannattaa sijoittaa fyysisesti jokaiseen luottavaan toimialueeseen. Kuva tällaisesta järjestelystä on pari sivua edempänä.

Esimerkki **Master domain -mallista**; toimialueet **ATK** ja **MYYNTI** luottavat toimialueeseen **HALLINTO**; sen yleinen **Domain Users**-ryhmä (**HALLINTO\Domain Users**) on otettu mukaan luottavien toimialueiden paikalliseen **Users**-ryhmään. Samoin on tehty **Domain Admins**-ryhmälle eli se on otettu mukaan paikallisiin **Administrators**-ryhmiin. Työasemat kuitenkin kuuluvat **ATK**- ja **MYYNTI**-toimialueisiin.



Paikallinen ryhmä (Local Group) on ryhmä, johon voi kuulua **paikallisia käyttäjiä** ja **yleisiä ryhmiä** (Global Group), mutta ei toisia paikallisia ryhmiä. **Yleinen ryhmä** näkyy luottosuhteen yli toisessakin toimialueessa; **toimialueen paikallinen käyttäjä** tai **paikallinen ryhmä** ei näy eikä sitä voida lisätä toisen toimialueen käyttäjäryhmiin.

Koska voit lisätä yleisiä käyttäjätunnuksia ja yleisiä käyttäjäryhmiä luottosuhteen yli luotetusta toimialueesta (*Master Domain*) luottavan toimialueen paikallisiin ryhmiin, voit esimerkiksi tehdä seuraavat operaatiot:

- Lisätä luotetusta toimialueesta (*Master Domain*) **Domain Admins-ryhmän** luottavan toimialueen paikalliseen Administrators-ryhmään. Tällöin käyttäjä kirjautuessaan luotetun toimialueen (*Master Domain*) käyttäjätunnuksellaan saa **luottavassa toimialueessa** paikallisen **Administrators-ryhmän** oikeudet **hallita luottavan toimialueen palvelimia**

- Lisätä luotetusta toimialueesta (*Master Domain*) **Domain Users-ryhmän** luottavan toimialueen paikalliseen Users-ryhmään. Tällöin käyttäjä kirjautuessaan luotetun toimialueen (*Master Domain*) käyttäjätunnuksellaan saa **luottavassa toimialueessa** paikallisen **Users-ryhmän** oikeudet **käyttää luottavan toimialueen palvelimia**.

Tässä taulukossa on esitetty ns. perinteisen, täysin keskitetyn mallin mukaiset käyttäjäryhmät edelläesitetyissä kolmessa toimialueessa:

Toimialue	Ryhmä	Ryhmän jäsenet
HALLINTO	Domain Admins	Kaikki HALLINTO-toimialueen pääkäyttäjät
HALLINTO	Administrators	HALLINTO-toimialueen Domain Admins-ryhmä
HALLINTO	Domain Users	Kaikki peruskäyttäjien käyttäjätunnukset
HALLINTO	Users	HALLINTO-toimialueen Domain Users-ryhmä

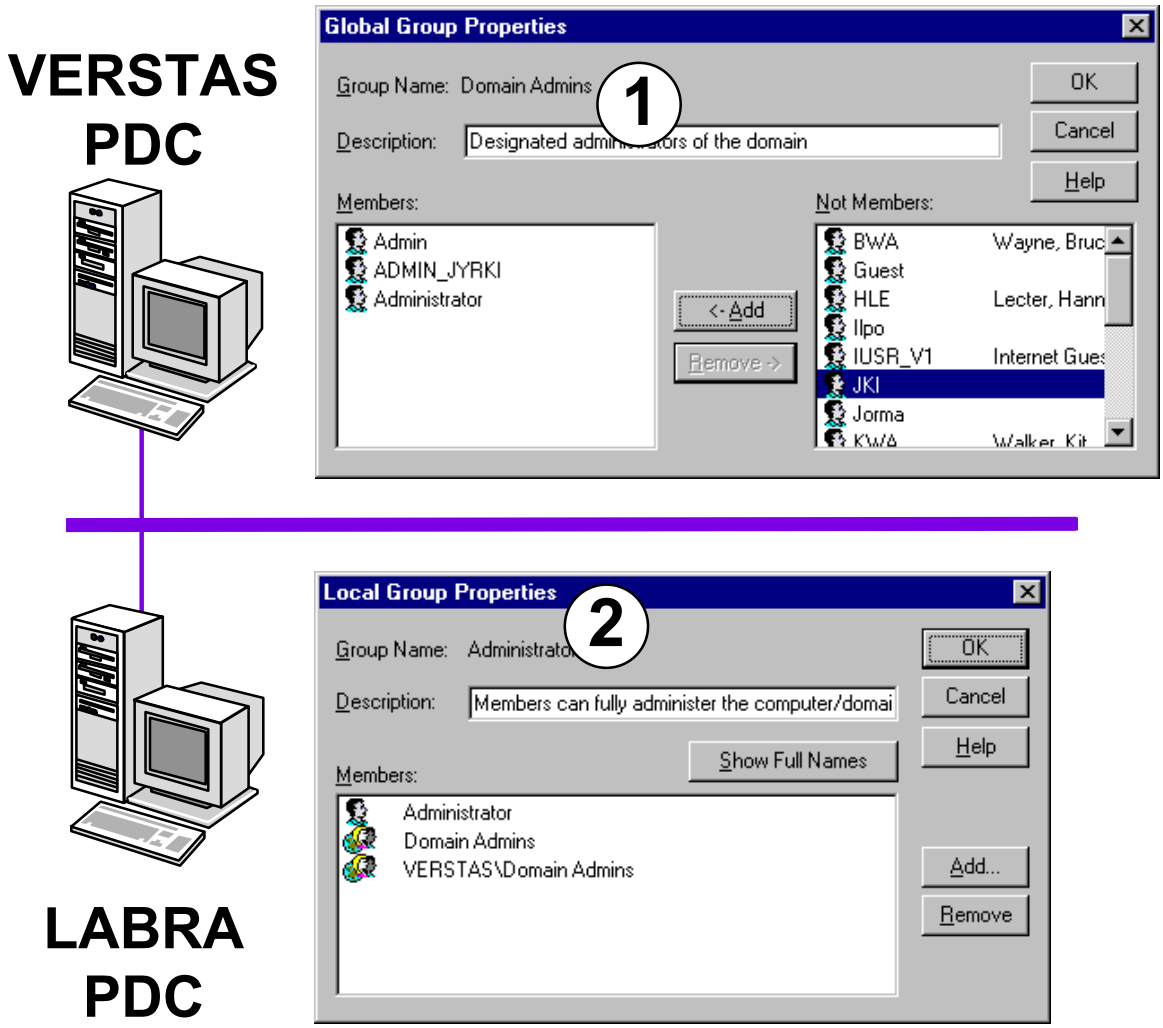
Toimialue	Ryhmä	Ryhmän jäsenet
ATK	Domain Admins	ATK-toimialueen Administrator-tunnus
ATK	Administrators	ATK-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä
ATK	Domain Users	-
ATK	Users	ATK-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä

Toimialue	Ryhmä	Ryhmän jäsenet
MYYNTI	Domain Admins	MYYNTI-toimialueen Administrator-tunnus
MYYNTI	Administrators	MYYNTI-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä
MYYNTI	Domain Users	-
MYYNTI	Users	MYYNTI-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä

Hieman ylimääräistä työtä tässä aiheuttaa se, että luottavan toimialueen NT-työasemissa käyttäjän oikeudet tulee määritellä erikseen, samoin kuin ne tehdään toimialueen sisälläkin. Esimerkiksi luotetun toimialueen käyttäjätunnus tulee lisätä luottavan toimialueen NT-työaseman paikalliseen ryhmään - tämäkään ei suinkaan tapahdu automaattisesti.

Toisaalta vahvuutena on mahdollisuus lisätä käyttäjätunnus esimerkiksi **Tehokäyttäjien** (Power Users) tai **Järjestelmänvalvojien** (Administrators) ryhmiin. Tällöin käyttäjä voi hallita vain *omaa* työasemaansa niin kuin parhaaksi näkee.

Seuraavaksi joitakin esimerkkejä eri tilanteista.

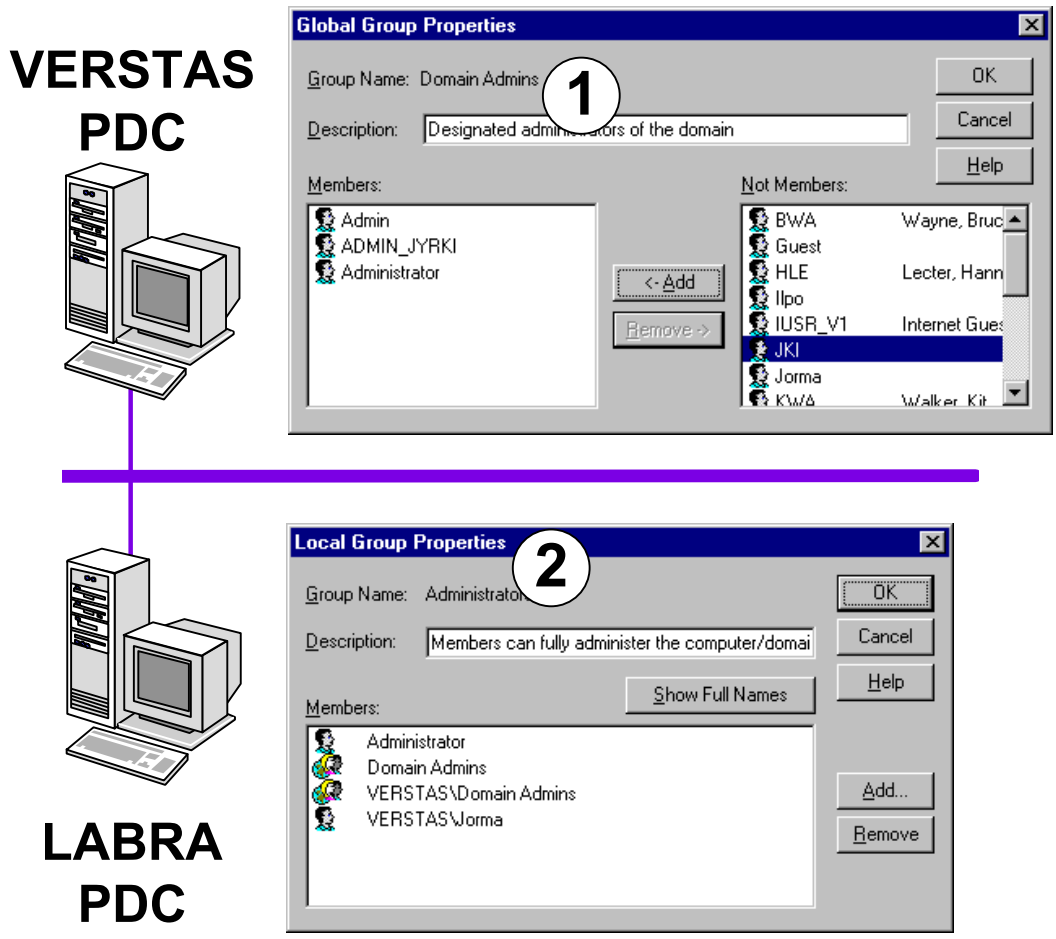


Tässä esimerkissä toimialueesta **LABRA** on yksisuuntainen luottosuhde toimialueeseen **VERSTAS**. **VERSTAS** on tällöin *Master Domain*, se on lutettu toimialue (*Trusted*) ja **LABRA** on luottava (*Trusting*). **VERSTAS**-

toimialueen **Domain Admins**-ryhmä on lisätty luottavan toimialueen paikalliseen **Administrators**-ryhmään. Tällöin käyttäjä kirjautuessaan luotetun toimialueen (*Master Domain*) käyttäjätunnuksella - **VERSTAS**-toimialueen **Admin**, **Administrator** tai **ADMIN_JYRKI** - saa **myös luottavassa toimialueessa** paikallisen **Administrators-ryhmän** oikeudet **hallita luottavan toimialueen palvelimia**. Kannattaa huomata, että **LABRA**-toimialueessa paikalliseen **Administrators-ryhmään** kuuluu mukaan myös **LABRA**-toimialueen **Administrator**-käyttäjätunnus sekä **LABRA**-toimialueen **Domain Admins**-ryhmä.

Seuraavassa esimerkissä **VERSTAS**-toimialueen käyttäjätunnus **Simo** on lisätty **LABRA**-toimialueessa paikalliseen **Administrators**-ryhmään (**2**), jolloin a.o. käyttäjä voi hallita **LABRA**-toimialueen palvelimia. **Simo** ei kuulu kuitenkaan **VERSTAS**-toimialueen **Domain Admins**-ryhmään (**1**), joten hän ei voi hallita **VERSTAS**-toimialueen palvelimia.

Tällainen tilanne tulee kyseeseen, jos **Simo** on vaikkapa **LABRA**-toimialueen tukihenkilö.



Jos halutaan, että **Simo** voi hallita **LABRA**-toimialueen palvelimien lisäksi **myös LABRA**-toimialueen NT-työasemia, niin tällöin **Simon** hallintaan kuuluvissa NT-työasemissa tulee jokaisessa lisätä **VERSTAS**-toimialueen käyttäjätunnus **Simo** erikseen NT-työaseman paikalliseen **Administrators**-ryhmään.

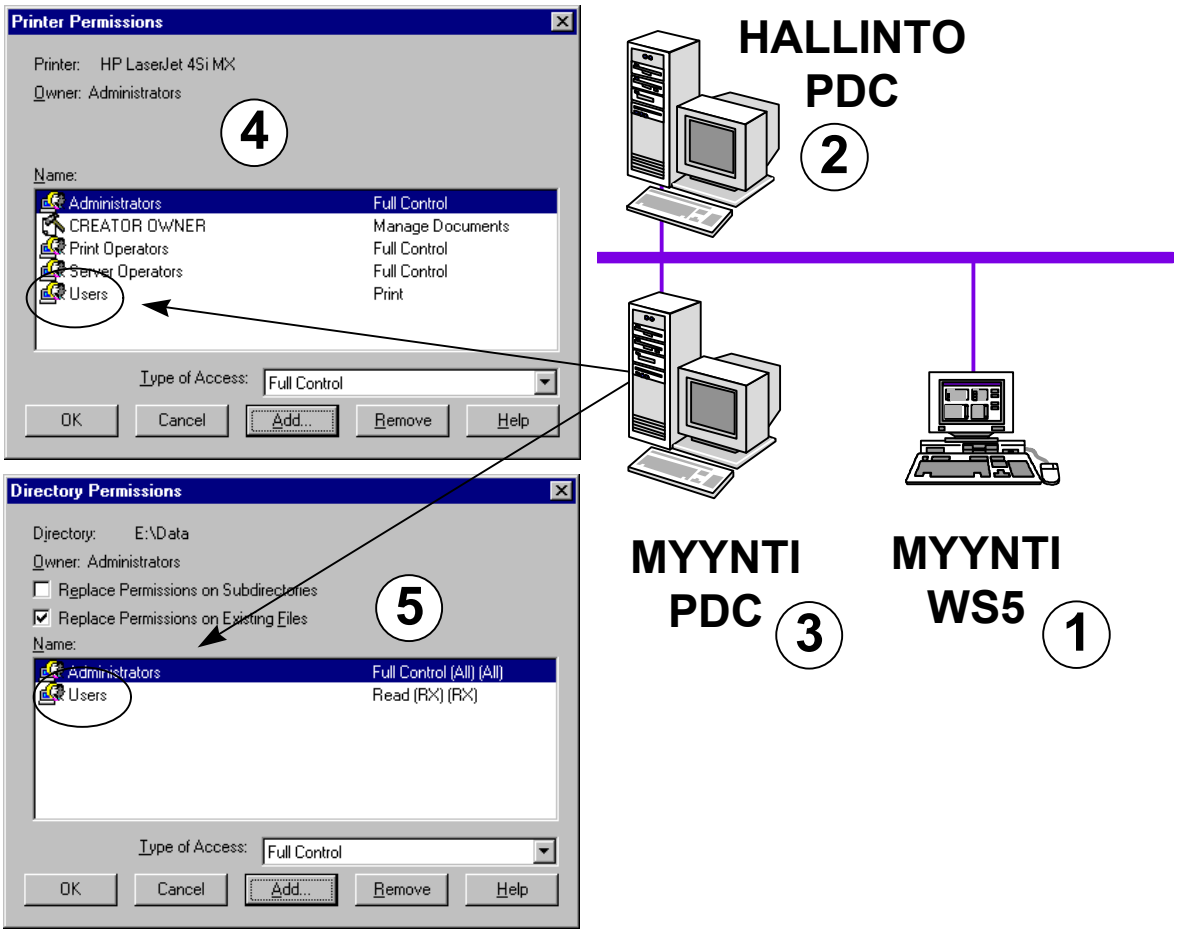
Toisaalta vahvuutena tässä on jälleen mahdollisuus lisätä käyttäjätunnus NT-työasemissa rajatusti esimerkiksi vain **Tehokäyttäjien** (Power Users) tai **Järjestelmänvalvojien** (Administrators) ryhmiin.

Kun ryhmäjäsenyydet ovat kunnossa, niin käyttäjien lisääminen ja käyttöoikeuksien myöntäminen on varsin joutuisaa.

Tässä esimerkissä ryhmäjäsenyydet ovat edellä esitetyn perusmallin mukaisia:

Toimialue	Ryhmä	Ryhmän jäsenet
HALLINTO	Domain Users	Kaikki HALLINTO-toimialueen pääkäyttäjät
MYYNTI	Users	HALLINTO-toimialueen Domain Users-ryhmä Admins-ryhmä

Kun käyttäjä kirjautuu **MYYNTI**-toimialueen NT-työasemassa **WS5** (**1**) käyttäjäksi **HALLINTO**-toimialueen **Domain Users**-ryhmän jäsenen käyttäjätunnuksella (**2**), hän saa samalla **Users**-ryhmän oikeudet **MYYNTI**-toimialueella (**3**). **MYYNTI**-toimialueen palvelin jakaa sekä kirjoittintaan verkkoon **MYYNTI**-toimialueen **Users**-ryhmälle tulostusoikeuksilla (**Print**),että DATA-hakemistoa **MYYNTI**-toimialueen **Users**-ryhmälle lukuoikeuksin (**Read**). Niinpä käyttäjä saa nämä oikeudet välittömästi käyttöönsä **HALLINTO**-toimialueen **Domain Users**-ryhmän jäsenen käyttäjätunnuksellaan.



Master Domain-mallissa ei muuten tyypillisesti ole ollenkaan NT- tai muitakaan työasemia itse *Master Domainissa*.

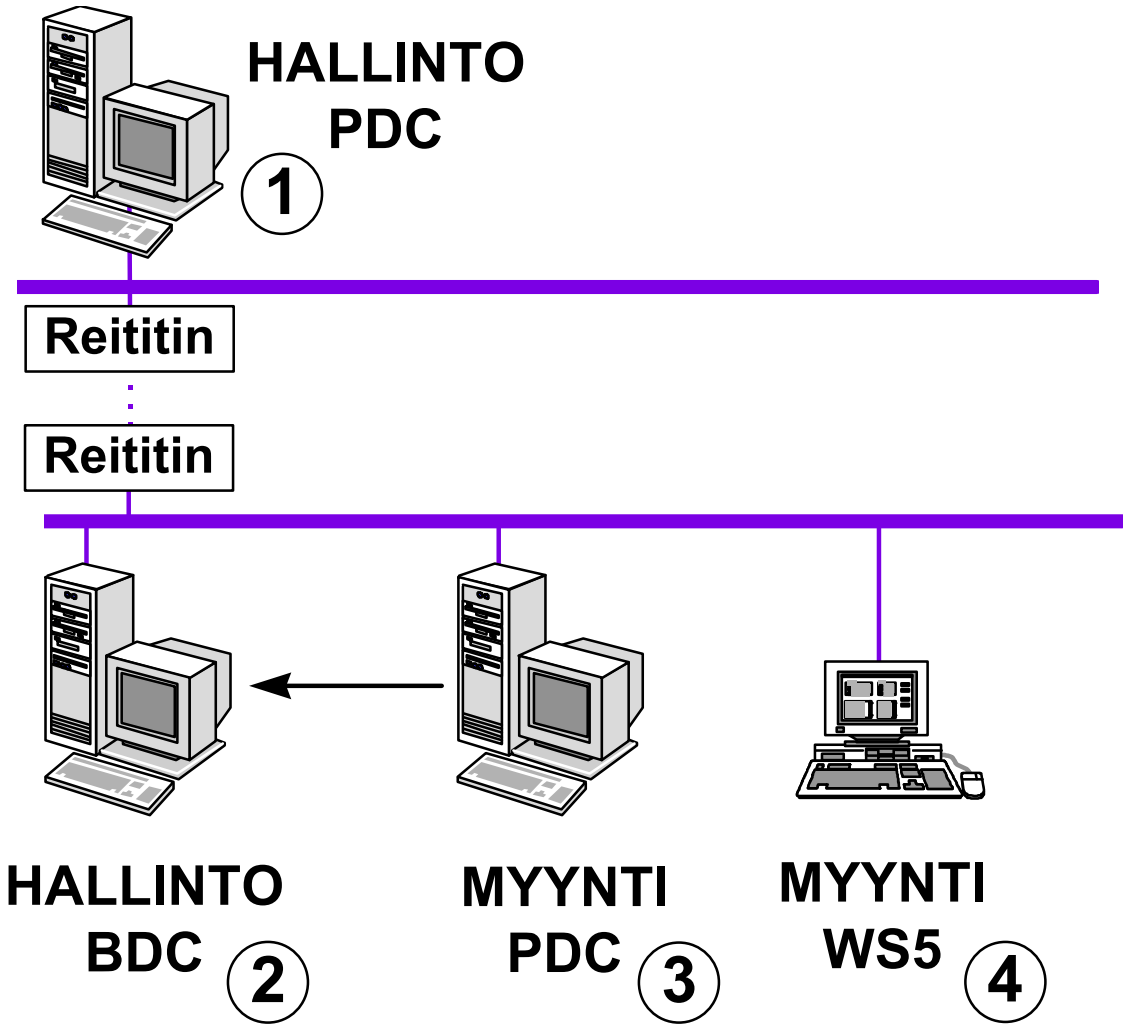
Master Domain-mallin jotkut ovat suomentaneet **päätoimialuemalliksi**.

Master domain -malli laajassa verkossa

Jos luottavat toimialueet ovat hitaan tietoliikenneyhteyden päässä, yksi luotetun toimialueen ohjauskone eli varapalvelin *(Backup Domain Controller)* kannattaa sijoittaa fyysisesti jokaiseen luottavaan toimialueeseen. Esimerkiksi **laajassa reititinverkossa** järjestetään tyypillisesti Master Domainin BDC samaan verkkoon kuin luottavan toimialueen PDC.

Tässä esimerkissä on yksisuuntainen luottosuhde **MYYNTI**-toimialueelta **HALLINTO**-toimialueelle. **HALLINTO**-toimialueen **PDC** (**1**)on fyysisesti etäällä (reititinverkon takana), mutta **HALLINTO**-toimialueen **BDC** (**2**)

on tuotu samaan aliverkkoon (ja vaikkapa segmenttiin) **MYYNTI**-toimialueen **PDC**:n (**3**) kanssa. Tässä tilanteessa luottosuhteen ylläpito tapahtuu **HALLINTO**-toimialueen **BDC**:n ja **MYYNTI**-toimialueen **PDC**:n välillä. Kun käyttäjä haluaa kirjautua **MYYNTI**-toimialueen NT-työasemasta **WS5** (**4**) **HALLINTO**-toimialueen käyttäjätunnuksella käyttäjäksi, **MYYNTI**-toimialueen **PDC** ohjaa kirjautumispyynnön **HALLINTO**-toimialueen **BDC**:lle, joka puolestaa hoitaa käyttäjän verkkoonkirjautumisen. Tässä se käyttää hyväkseen käyttäjätietokantansa kopiota.



Jos **yhteys katkeaa** *Master Domainin* PDC:hen, niin Master Domainin BDC kuitenkin on se, joka hyväksyy/hylkää käyttäjien verkkoonkirjautumispyynnöt. Ongelmia tulee vasta siinä vaiheessa, kun halutaan tehdä muutoksia *Master Domainin* käyttäjätietokantaan - se ei onnistu ennen kuin PDC:hen on jälleen yhteys.

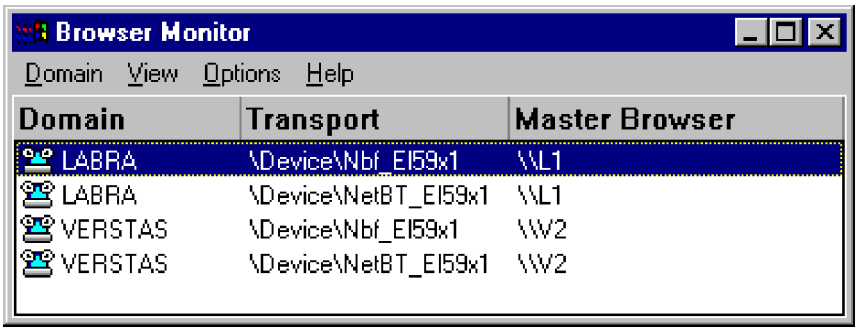
Muista seuraavat seikat:

- Pyri käyttämään kaikissa Domain Controller-palvelimissa samoja Windows NT -versioita (esim. joko 3.51 tai 4.0)

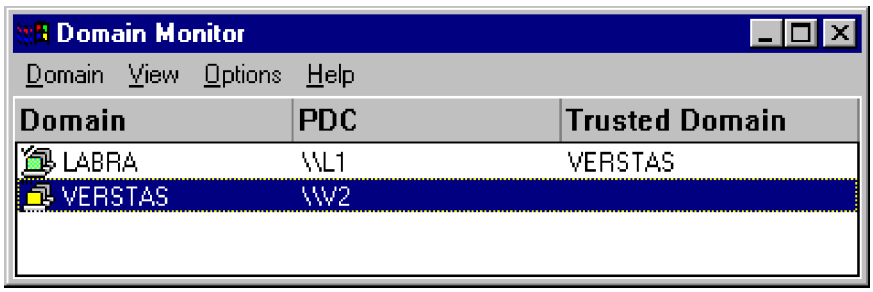
- Pyri päivittämään **Service Packit** tarvittaessa jotakuinkin saman aikaisesti palvelimiin

- Luo ja päivitä tarvittaessa **LMHOSTS**-tiedostot kaikkiin palvelimiin. Niissä tulisi olla kaikkien PDC- ja tärkeimpien BDC-palvelimien nimet ja osoitteet

- **Selauspalvelu** (Browser) voi toimia omituisesti laajassa reitittinverkossa. Pyri pitämään työasemissa (Windows 95, Työryhmä-Windows 3.11) työryhmien nimet samoina kuin toimialueiden nimet. Selauspalvelu vaatii toimiakseen reitittimen yli **UDP-portin 137** avaamisen. Valvo selauspalvelua Resource Kitin **Browser Monitor**-ohjelmalla



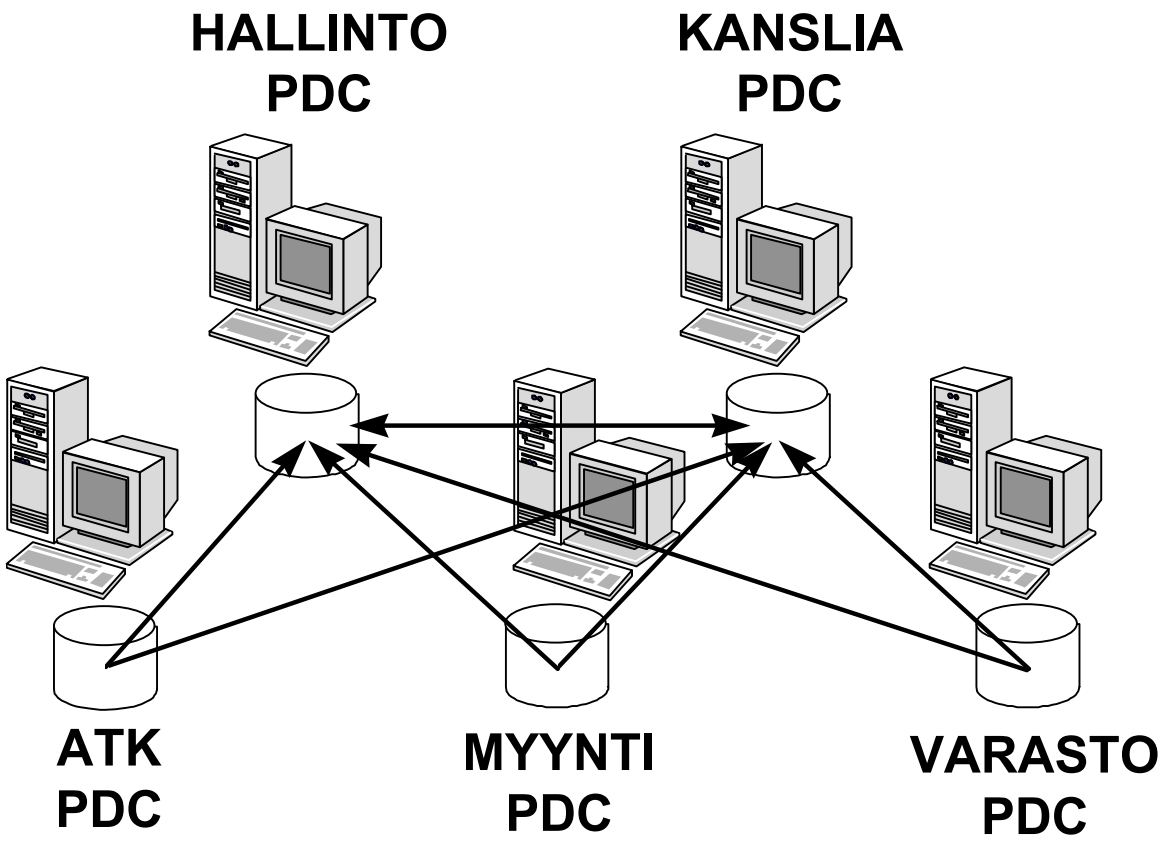
- Valvo toimialueiden välisiä luottosuhteita Resource Kitin **Domain Monitor**-ohjelmalla!



Multiple master domain

Luottosuhde voi olla myös **kaksisuuntainen** (*Two-way trust*); molemmat toimialueet voivat luottaa toisiinsa. Luottosuhde ei ole kuitenkaan läpinäkyvä eli toimialueen läpi se ei voi ulottua. Luottosuhde pitää aina erikseen perustaa sekä luottavassa että luotetussa toimialueessa.

Multiple master domain -malli on "laajennettu" **Master domain** -malli; käytetään kahta tai useampaa *Master domainia*, jotka luottavat toisiinsa. Toimialue **ZZZ** luottaa toimialueisiin **NNN** ja **YYY**, jotka vastaavasti luottavat molemmat toisiinsa. Näin voidaan erittäin suurissa verkoissa tukea lähes rajatonta käyttäjämäärää, koska aina tarvittaessa voidaan lisätä uusi *master domain*.



Tässä esimerkissä toimialueet **ATK**, **MYYNTI** ja **VARASTO** luottavat toimialueisiin **HALLINTO** ja **KANSLIA**, jotka vastaavasti luottavat molemmat toisiinsa (kaksisuuntainen luottosuhde). Master domaineita tässä mallissa ovat sekä **HALLINTO**- että **KANSLIA**-toimialueet.

Tässä taulukossa on esitetty ns. perinteisen, täysin keskitetyn mallin mukaiset käyttäjäryhmät edelläesitetyissä viidessä toimialueessa.

Master Domainit:

Toimialue	Ryhmä	Ryhmän jäsenet
HALLINTO	Domain Admins	Kaikki HALLINTO-toimialueen pääkäyttäjät
HALLINTO	Administrators	HALLINTO-toimialueen Domain Admins-ryhmä, KANSLIA-toimialueen Domain Admins-ryhmä
HALLINTO	Domain Users	Kaikki peruskäyttäjien käyttäjätunnukset
HALLINTO	Users	HALLINTO-toimialueen Domain Users-ryhmä, KANSLIA-toimialueen Domain Users-ryhmä

Toimialue	Ryhmä	Ryhmän jäsenet
KANSLIA	Domain Admins	Kaikki KANSLIA-toimialueen pääkäyttäjät
KANSLIA	Administrators	KANSLIA-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä
KANSLIA	Domain Users	Kaikki peruskäyttäjien käyttäjätunnukset
KANSLIA	Users	KANSLIA-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä

Luottavat toimialueet:

Toimialue	Ryhmä	Ryhmän jäsenet
ATK	Domain Admins	ATK-toimialueen Administrator-tunnus
ATK	Administrators	ATK-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä, KANSLIA-toimialueen Domain Admins-ryhmä
ATK	Domain Users	-
ATK	Users	ATK-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä, KANSLIA-toimialueen Domain Users-ryhmä

Toimialue	Ryhmä	Ryhmän jäsenet
MYYNTI	Domain Admins	MYYNTI-toimialueen Administrator-tunnus
MYYNTI	Administrators	MYYNTI-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä, KANSLIA-toimialueen Domain Admins-ryhmä
MYYNTI	Domain Users	-
MYYNTI	Users	MYYNTI-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä, KANSLIA-toimialueen Domain Users-ryhmä

Toimialue	Ryhmä	Ryhmän jäsenet
VARASTO	Domain Admins	VARASTO-toimialueen Administrator-tunnus
VARASTO	Administrators	VARASTO-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä, KANSLIA-toimialueen Domain Admins-ryhmä
VARASTO	Domain Users	-
VARASTO	Users	VARASTO-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä, KANSLIA-toimialueen Domain Users-ryhmä

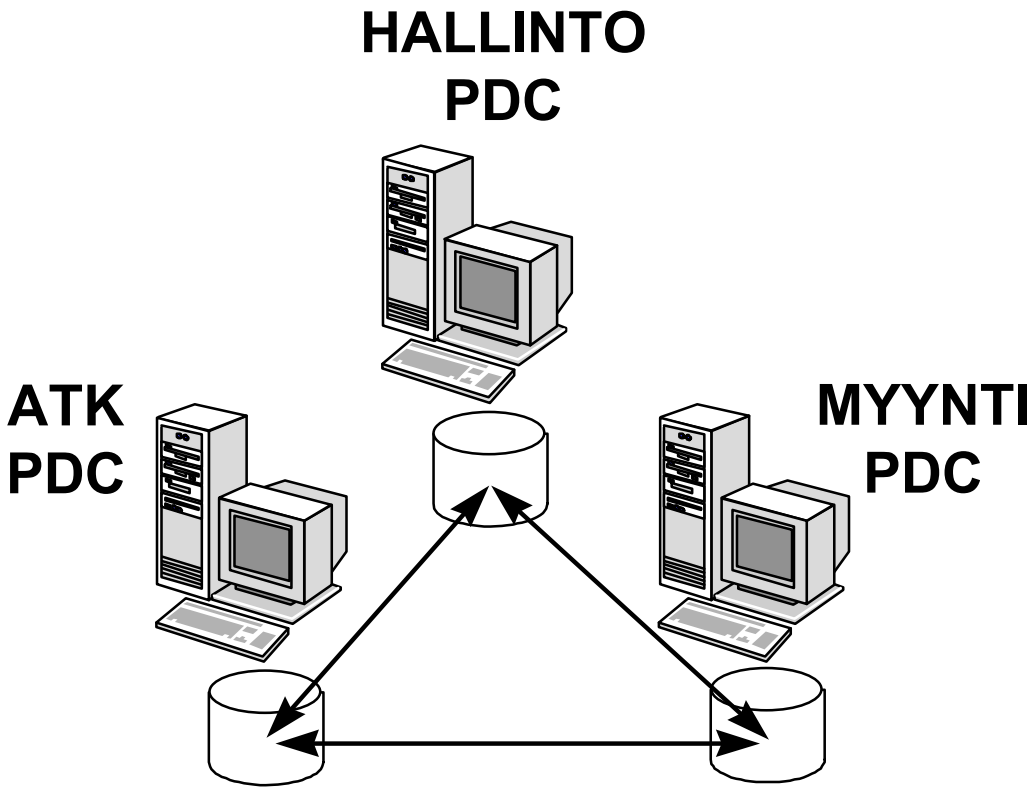
Multiple master domain -mallista jotkut asiantuntijat tarjoavat suomennosta Monen päätoimialueen malli .

Complete Trust

Kaksisuuntaisilla luottosuhteilla voidaan luoda luottosuhde, jossa kaikki toimialueet luottavat toisiinsa. Tämä on ns. **täydellinen luottosuhde** (*Complete Trust*). Complete trust -mallissa kaikki toimialueet luottavat toisiinsa.

Lisäksi voidaan luoda erilaisia sekamalleja, mutta tällöin on syytä miettiä käyttäjätunnukset ja niiden oikeudet vielä kerran!

Complete trust -mallista jotkut asiantuntijat tarjoavat suomennosta Täyden luottamuksen malli .



Tässä on esitetty Complete trust -mallin mukaiset ryhmät täydellisine jäsenyyksineen. Administrators-ryhmien jäsenyyksiä toki kannattaa soveltaa; ei ehkä liene tarpeen kaikkien toimialueiden pääkäyttäjien päästä hallinnoimaan kaikkien toimialueiden palvelimia, vaikka tässä mallissa sekin on mahdollista.

Toimialue	Ryhmä	Ryhmän jäsenet
HALLINTO	Domain Admins	Kaikki HALLINTO-toimialueen pääkäyttäjät
HALLINTO	Administrators	HALLINTO-toimialueen Domain Admins-ryhmä, MYYNTI-toimialueen Domain Admins-ryhmä, ATK-toimialueen Domain Admins-ryhmä
HALLINTO	Domain Users	Kaikki peruskäyttäjien käyttäjätunnukset
HALLINTO	Users	HALLINTO-toimialueen Domain Users-ryhmä, MYYNTI-toimialueen Domain Users-ryhmä, ATK-toimialueen Domain Users-ryhmä

Toimialue	Ryhmä	Ryhmän jäsenet
ATK	Domain Admins	ATK-toimialueen Administrator-tunnus
ATK	Administrators	ATK-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä, MYYNTI-toimialueen Domain Admins-ryhmä
ATK	Domain Users	-
ATK	Users	ATK-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä, MYYNTI-toimialueen Domain Users-ryhmä

Toimialue	Ryhmä	Ryhmän jäsenet
MYYNTI	Domain Admins	MYYNTI-toimialueen Administrator-tunnus
MYYNTI	Administrators	MYYNTI-toimialueen Domain Admins-ryhmä, HALLINTO-toimialueen Domain Admins-ryhmä, ATK-toimialueen Domain Admins-ryhmä
MYYNTI	Domain Users	-
MYYNTI	Users	MYYNTI-toimialueen Domain Users-ryhmä, HALLINTO-toimialueen Domain Users-ryhmä, ATK-toimialueen Domain Users-ryhmä

Toimialuemallin suunnittelu

Windows NT **3.51**:n Resource Kitin mukana tuleva **Domain Plannerin** avulla voi yrittää suunnitella omaan ympäristöön sopivaa toimialuemallia. Windows NT 4.0:n Resource Kiteissä tätä ohjelmaa ei enää ole mukana.

Suunniteltaessa omaa toimialuemallia tulisi pohtia seuraavia asioita:

- Palvelinten sijoittelu ja hallinta
- Työasemien sijoittelu ja hallinta
- Työasemien ja palvelimien väliset maantieteelliset etäisyydet, tietoliikenneyhteyksien järjestäminen.

Useita eri toimialueita voidaan tarvita eri syistä:

- Organisatoriset syyt:
  - Kustannuspaikat
  - Paikallinen tuki
  - Toiminnan erilaisuus eri yksiköissä
- Maantieteelliset syyt: etäisyydet resurssien ja käyttäjien välillä
- Ongelmalliset linjayhteydet
- Tietoturvasta ja esimerkiksi Internet-yhteyksistä johdetut syyt.

Käyttäjätietokannan koko

Yksi asia suunniteltaessa toimialuemalleja on käyttäjätietokannan koko. On syytä muistaa, että jokainen tunnus vie käyttäjätietokannasta tilaa. Tunnuksia on käyttäjillä, ryhmillä ja NT-koneilla.

Jokainen käyttäjätunnus vie 1024 tavua ja jokainen NT-konetunnus vie 512 tavua. Paikallinen ryhmä (*Local Group*) vaatii 512 tavua sekä 36 tavua jokaista ryhmän jäsentä kohti. Yleinen ryhmä (*Global Group*) vie 512 tavua sekä 12 tavua jokaista ryhmän jäsentä kohti. Ero selittyy sillä, että yleisen ryhmän jäsenet ovat kaikki käyttäjätunnuksia samassa toimialueessa; paikallisessa ryhmässä on tallennettu myös tieto käyttäjätunnuksen toimialueesta (joka voi luottosuhteen kautta olla toinenkin toimialue),

Suurin käyttäjätietokannan koko on ollut tiettävästi 40 megatavua.

Jos luodaan esimerkiksi **WWWUsers** -niminen paikallinen ryhmä, johon lisätään 800 käyttäjää, se vie 29312 tavua. Jos sen sijaan luodaan yleinen ryhmä vaikkapa nimeltä **VERSTAS_WWWUsers**, joka lisätään paikalliseen **WWWUsers** -nimiseen ryhmään, tilaa menee käyttäjäein ryhmäjäsenyyteen 10112 tavua sekä 512 + 36 tavua paikallisen ryhmän jäsenyyteen. Ero on 18652 tavua.

Esimerkkitaulukko käyttäjätietokannan koosta:

Käyttäjätunnusten lkm	NT-koneiden lkm	Ryhmien lkm	Käyttäjätietokanta
2000	2000	40	3,02 Mt
5000	5000	100	7,55 Mt
10000	2000	200	11,20 Mt
20000	5000	200	22,89 Mt
20000	20000	200	30,21 Mt
39000	100	200	39,92 Mt

Viimeisen rivin esimerkki selittyy sillä, että kyseessä on Master Domain-mallin Master Domain, jossa ei ole NT-konetunnuksia - ne kuuluvat resurssitoimialueisiin.

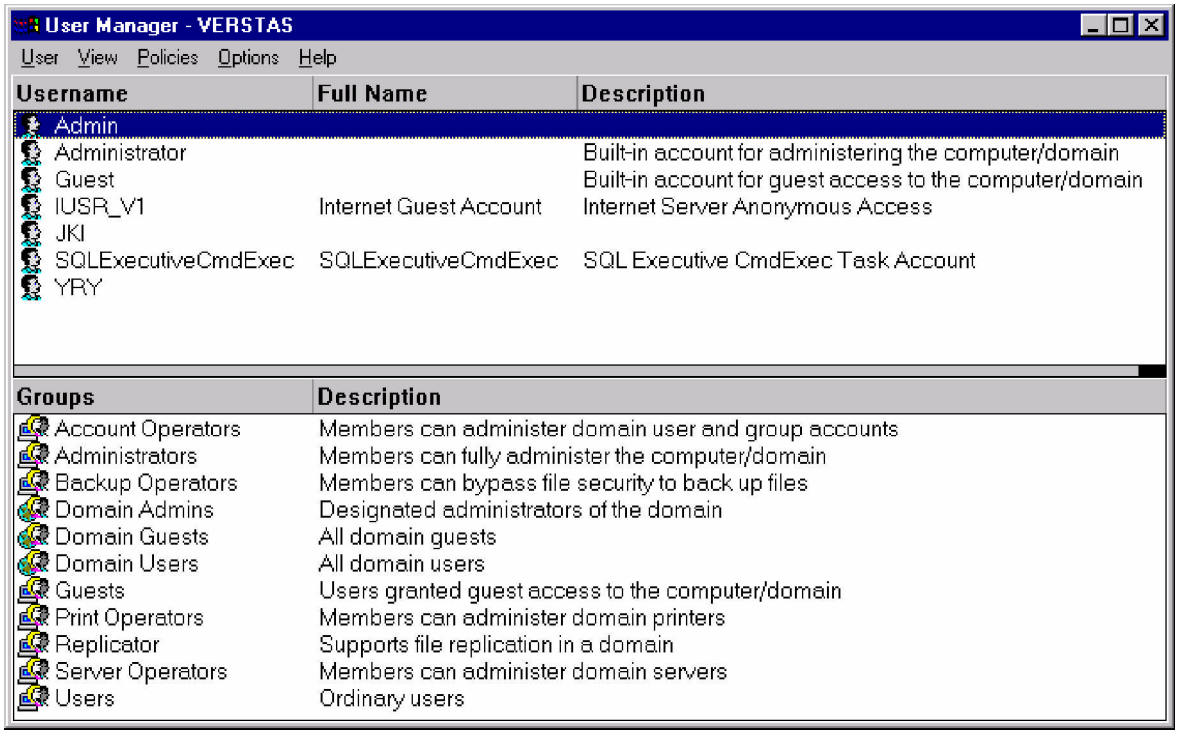
User Manager for Domains

Windows NT -palvelimien mukana tulee **User Manager for Domains**, jolla voi hallita Windows NT -palvelimen muodostaman **toimialueen** (*domain*) **keskitettyä käyttäjätietokantaa** sekä minkä tahansa **Windows NT -työaseman käyttäjätietokantaa**.

Pääasiassa **User Manager for Domainsia** toki käytetään toimialueen keskitetysti hallittujen käyttäjätunnusten hallinnointiin.

Microsoft on suomentanut käyttäjätunnuksen **käyttäjätiliksi** (User Account). Sen voidaan katsoa sisältävän muutakin informaatiota kuin pelkästään käyttäjän kirjautumisen yhteydessä antaman tunnuksen.

Käyttäjälle asetettavat ominaisuudet eroavat siinä, onko kyseessä **Käyttäjien hallinta** (User Manager) vai **User Manager for Domains** - pääasiassa alareunan painikkeet eroavat siten, että **Käyttäjien hallinnassa** (User Manager) ei voi määritellä kaikkea sellaista mitä **User Manager for Domainsissa** voi käyttäjälle määritellä. Tämä johtuu siitä, että Käyttäjien hallinnalla (User Manager) voi luoda vain työaseman paikallisia käyttäjätunnuksia.

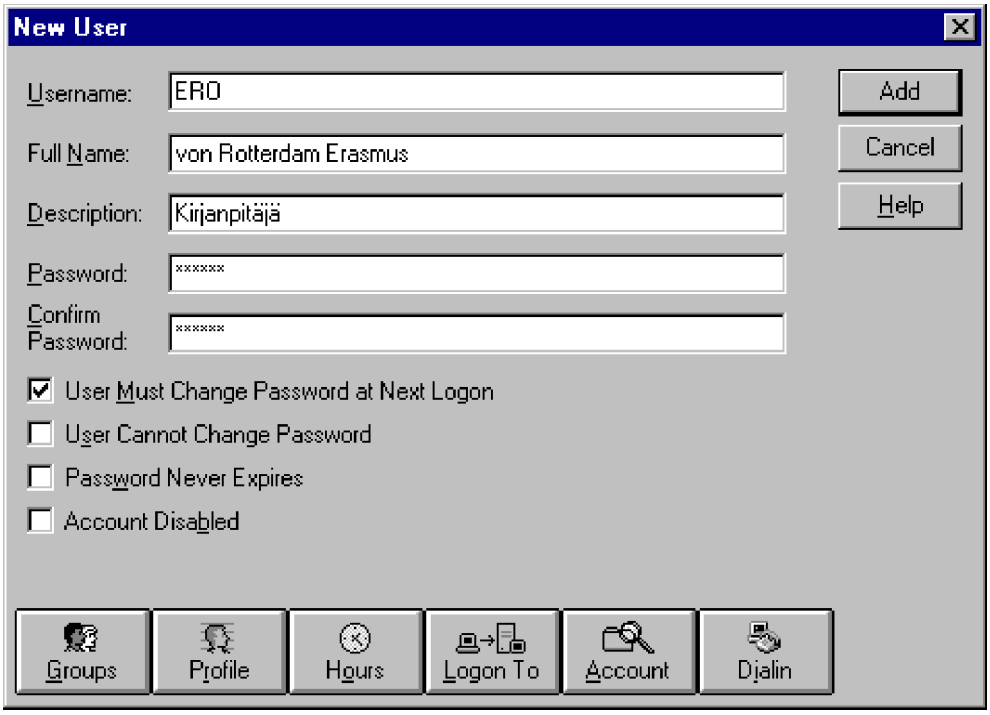


User Manager for Domainsin yläosassa näkyvät käyttäjätilit ja alaosassa

käyttäjäryhmät. Jos käytät ohjelmaa hitaan linjayhteyden (esim. RAS) yli, niin valitse **Options** | **Slow Speed Connection**. Oikean reunan mustasta vaakasuorasta palkista voit venyttää ikkunoiden suhteellista kokoa.

Uuden käyttäjätunnuksen luominen

Uusi käyttäjä luodaan **User Manager for Domainsilla** valitsemalla **User** | **New User**.



Anna asetukset seuraavasti:

1) Kirjoita **Username**-ruutuun enintään 20 merkin pituinen käyttäjätunnus. Millään muulla hallittavan toimialueen tai työaseman käyttäjällä tai ryhmällä ei saa olla samaa nimeä. Nimessä ei saa olla seuraavia merkkejä:

" / \ [ ] : ; | = , + * ? < >

Käyttäjänimi on ainoa **pakollinen** tieto käyttäjästä!

2) Kirjoita **Full Name** -ruutuun käyttäjän koko nimi.

3) Kirjoita **Description**-ruutuun käyttäjän tai käyttäjätilin kuvaus

4) Kirjoita salasana **Password**- ja vahvista salasana **Confirm Password** -ruudussa, anna enintään 14 merkin pituinen salasana. Salasanojen kirjainkoko on merkitsevä - NT erottelee isot ja pienet kirjaimet

5) Valitse tarvittaessa tilin poistaminen käytöstä **Account Disabled** tai poista sen valinta. Tee myös salasanamääritykset: käyttäjän on muutettava salasana seuraavalla kirjautumiskerralla **User Must Change Password at Next Logon**, jos käyttäjän halutaan antavan oma salasanansa tai käyttäjä ei voi muuttaa salasanaa valinnalla **User Cannot Change Password**, jos halutaan pitää nyt annettu salasana. Salasana ei vanhene valinnalla **Password Never Expires** - valitse tämä, jos halutaan että NT ei pakota käyttäjää vaihtamaan jossain vaiheessa salasanaansa. Vaihtoehdot **User Must Change Password at Next Logon** ja **User Cannot Change Password** eivät voi olla samanaikaisesti voimassa!

6) Ikkunan alareunassa on painikkeita, joiden avulla voit määrittää lisäominaisuuksia. Valitse haluamasi painike ja tee tarvittavat määritykset valintaikkunassa: jos hallittavana kohteena on NT-työasema, vain **Ryhmät** (Groups), **Profiili** (Profile) ja **Puhelinyhteys** (Dialin) ovat käytettävissä. Jos hallittavana kohteena on toimialue, käytettävissä ovat seuraavat kuusi painiketta: **Groups**, **Profile**, **Hours**, **Logon To**, **Account** ja **Dialin**.

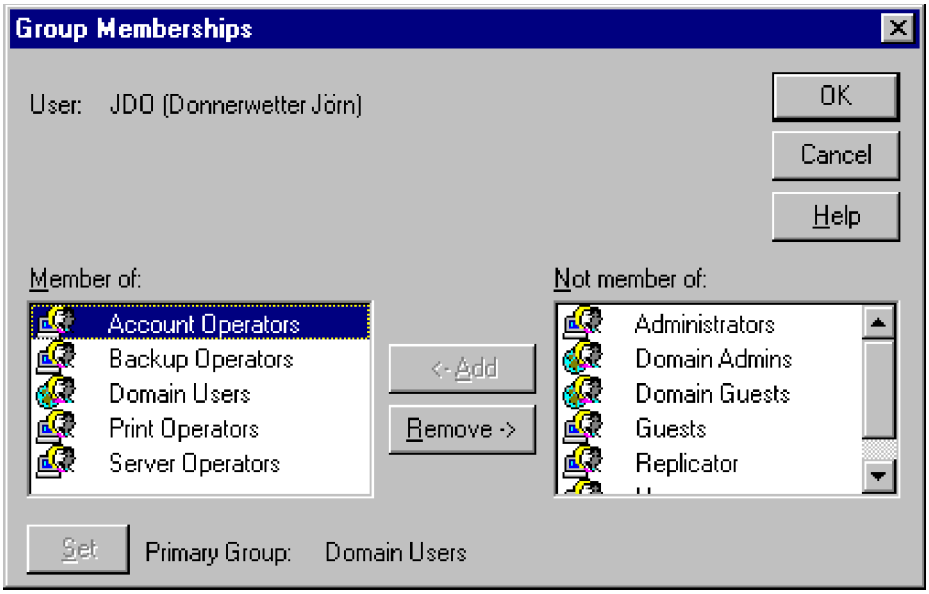
7) Valitse lopuksi **Add**-painike. Käyttäjätili lisätään ja ikkunaan palautuu oletusarvot.

Jos haluat lisätä useita käyttäjätilejä, toista vaiheet 1 - 7; kun lopetat uusien käyttäjien luomisen, valitse lopuksi **Close**.

Ryhmäjäsenyydet

Painikkeella **Groups** saat **Group Memberships**-valintaikkunan, jonka avulla voit hallita käyttäjätilien jäsenyyksiä toimialueen tai työaseman ryhmissä.

Ryhmät **User Manager for Domainsissa**:



Lisää käyttäjätunnus yhteen tai useampaan ryhmään valitsemalla yksi tai useampi ryhmä **Not Member of** -ruudusta ja valitse **Add**-painike; voit myös valita useamman ryhmän ja vetää valittujen ryhmien kuvakkeet **Member of** -ruutuun.

Vastaavasti voit poistaa jäsenyyden valitsemalla **Remove**-painikkeen. Ensisijaista ryhmää **Primary Group** ei kuitenkaan voi poistaa; muuta käyttäjätunnuksen ensisijaista ryhmää valitsemalla jokin yleinen ryhmä **Member of** -ruudusta ja painamalla sitten **Set**.

Ensisijainen ryhmä on se, mihin käyttäjän oikeustasoa ensin verrataan.

Tavallisesti ei ole mitään syytä siihen, että sama käyttäjätunnus on jäsenenä sekä järjestelmänvalvojien että käyttäjien ryhmissä. Luo omat käyttäjätunnukset järjestelmänvalvojia ja käyttäjiä varten!

Valitse lopuksi **OK**.

Käyttäjäprofiilit

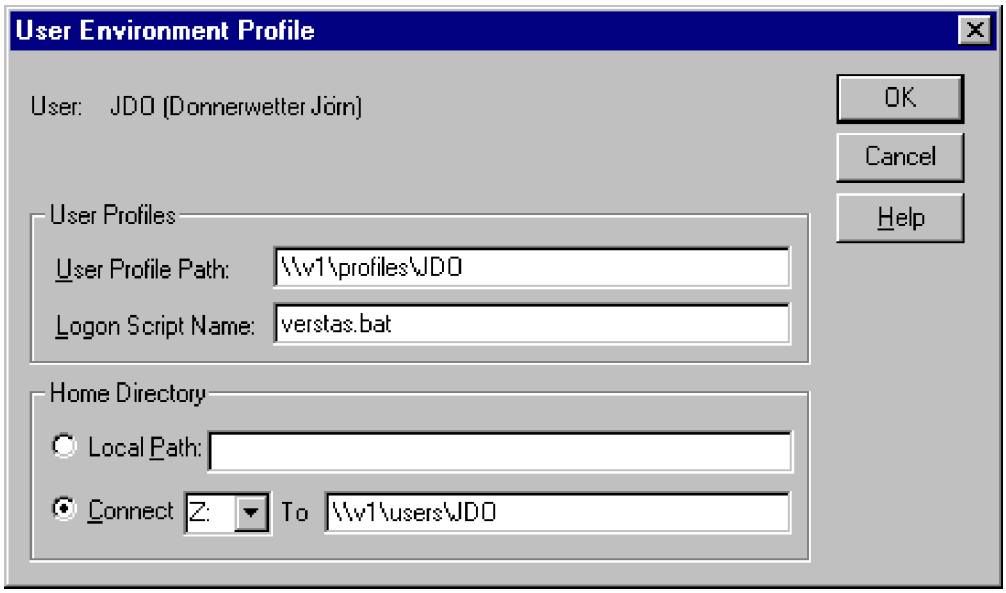
User Environment Profile -valintaikkunan avulla määritetään käyttäjäprofiili, kirjauskomentosarja ja käyttäjätunnuksen kotihakemisto; nämä määritykset ovat valinnaisia.

Profiilin asetuksia määritellään paitsi **User Manager for Domainsissa**, myös **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen **Käyttäjäprofiilit** (User Profiles)-välilehdessä.

Oikein käytettyinä profiilit ovat erittäin tehokas keino keskittää käyttäjän ympäristön hallinta!

Profiileita on käsitelty kirjassa myös hieman tuonnempana enemmän.

Profiilin asetukset **User Manager for Domainsissa**:



Käyttäjän profiili asetetaan **User Profile Path**-kohdassa. Jos sitä ei määritellä, se voi olla **paikallinen** (*Local*), eli sijaita vain NT-työaseman paikallisessa **Profiles**-järjestelmähakemistossa. Jos se määritellään, se voi sijaita **palvelimella** (*Roaming*). Jos haluat määritellä käyttäjälle **palvelimella sijaitsevan** (*Roaming*) profiilin, määritä käyttäjäprofiilin sijainti kirjoittamalla sen polku **Käyttäjäprofiilin polku** (User Profile Path) -ruutuun; polun on oltava **verkkopolku** annettuna UNC-nimellä, esimerkiksi **\\V1\PROFILES\JKI**.

Lisäksi mahdollisen Windows NT 4.0-työasemassa jo sijaitseva **paikalli-**

sen (*Local*) profiilin tyyppi ja sijainti on muutettava Windows NT 4.0-työasemassa **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen avulla. **Käyttäjäprofiilit** (User Profiles)-välilehden **Muuta tyyppi** (Change Type)- ja **Kopioi mihin** (Copy To)-painikkeilla voit muuttaa profiilin tyyppiä ja sijaintia.

Itse käyttäjän profiili sisältää kaksi osaa:

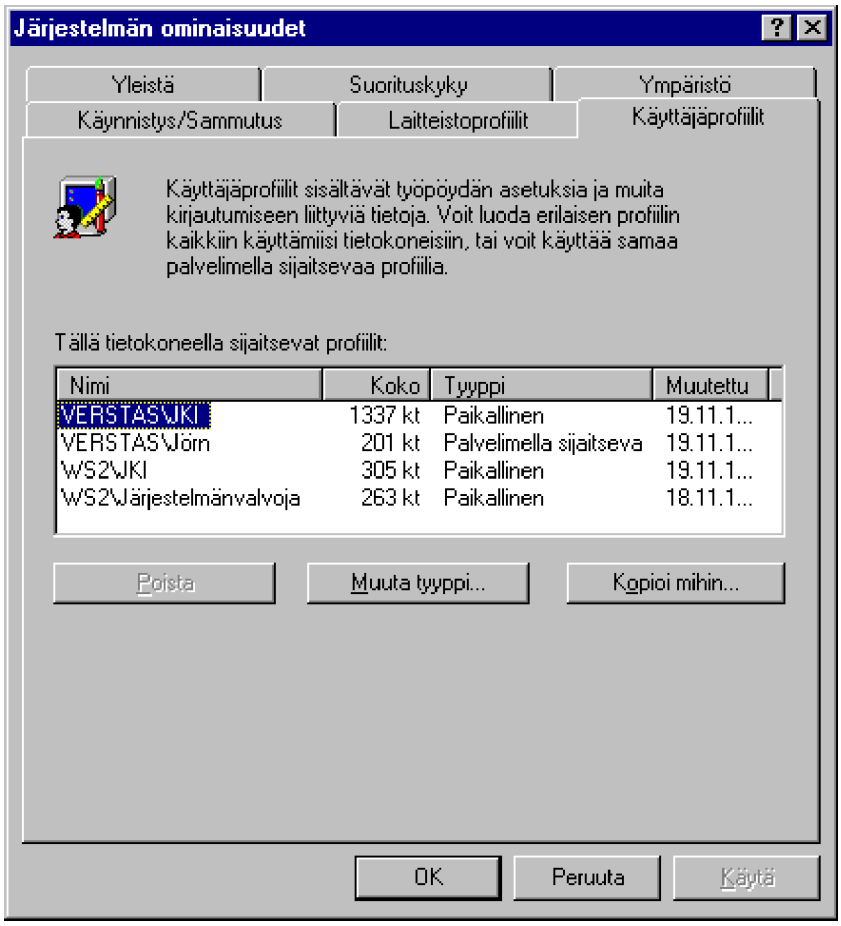
1) Järjestelmäkansiot (*folder*), jotka sijaitsevat **Profiles-**järjestelmähakemistossa (**\%Systemroot%\Profiles**, esimerkiksi työasemassa **C:\Winnt\Profiles**). Alihakemistoista tärkeimmät ovat **\Desktop** - käyttäjän työpöytä, **\Recent** - lista viimeksi käsitellyistä tiedostoista, **\SendTo** - hiiren pikavalikon Lähetä-valinta ja **\StartMenu** on käynnistyksessä suoritettavien ohjelmien kansio. Näitä voi käsitellä tarvittaessa suoraan **Käynnistä** (Start)-valikosta. Lisäksi on joitakin **piilotettuja** hakemistoja: verkkoympäristö **\NetHood**, kirjoittimet **\PrintHood** ja mallit **\Templates**. Jos sekä Windows NT -työaseman **paikallinen käyttäjätunnus** että Windows NT -toimialueella määritellyt käyttäjätunnukset ovat samat, niin työaseman hakemistorakenteeseen tulee kaksi käyttäjätunnuksen mukaista hakemistoa, esimerkiksi **JKI** ja **JKI.000**.

2) Tiedosto **NTUser.dat** on käyttäjätunnuksen mukaisessa **Profiles**-järjestelmähakemiston alihakemistossa. Profiiliitiedostoon **NTUser.dat** tallennetaan seuraavat asetukset: **Resurssienhallinta** (Explorer), **Tehtäväpalkki** (Taskbar), **Kirjoittimen** asetukset, **Ohjauspaneeli** (Control Panel), **Apuohjelmien** asetuksia ja **Opasteen** kirjanmerkit. Profiilitiedoston tiedostonimi voi olla henkilökohtaisen profiilin (**NTUser.dat**) tai pakollisen käyttäjäprofiilin (**NTUser.man**) nimi.

NT-työasemassa **aiemmin** kirjautuneiden käyttäjien profiilit tyyppeineen näet **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen **Käyttäjäprofiilit** (User Profiles)-välilehdessä.

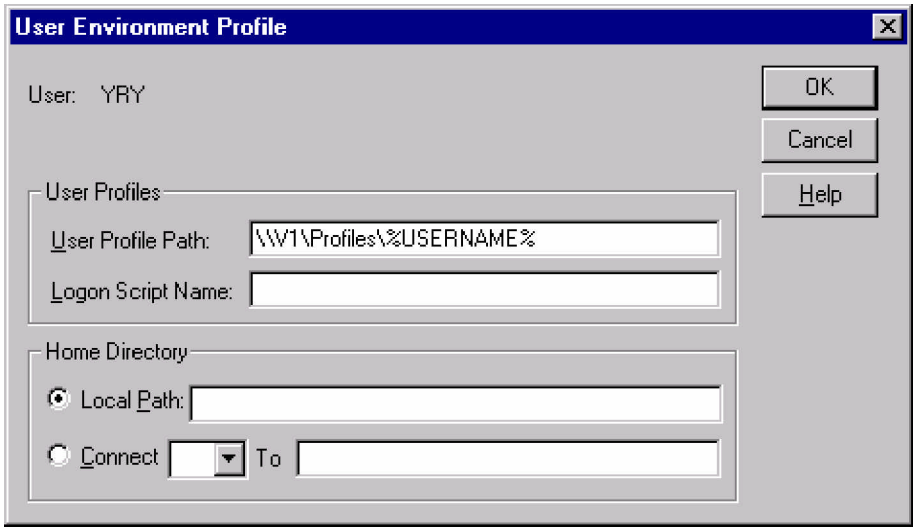
Käyttäjän profiilin sijaintia et voi kuitenkaan muuttaa esimerkiksi Resurssienhallinnalla. Sen sijaan **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen **Käyttäjäprofiilit** (User Profiles)-välilehdessä **Muuta tyyppi** (Change Type)- ja **Kopioi mihin** (Copy To)-painikkeilla voit muuttaa profiilin tyyppiä ja sijaintia.

Tätä menettelyä kannattaa käyttää, jos käyttäjällä on jo työasemassaan mukava työskentely-ympäristö ja siitä halutaan tehdä **palvelimella sijaitsevan** (*Roaming*) profiili. Valitse profiili, paina **Kopioi mihin** (Copy To)-painiketta ja valitse kohteeksi käyttäjän palvelimella sijaitseva profiilin hakemisto - sama mikä on käyttäjälle annettu **Käyttäjien hallinnassa** (User Manager) tai **Toimialueen käyttäjien hallinnassa** (User Manager for Domains).

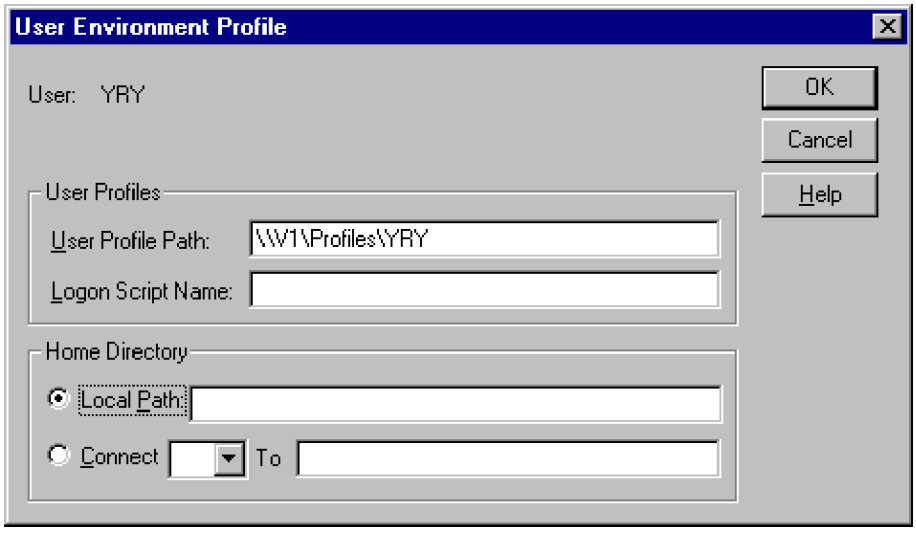


Jos luot useammalle käyttäjälle profiilin samalla kertaa, **voit korvata** profiifin sijainnin ympäristömuuttujasta saatavalla käyttäjänimellä **%USERNAME%**.

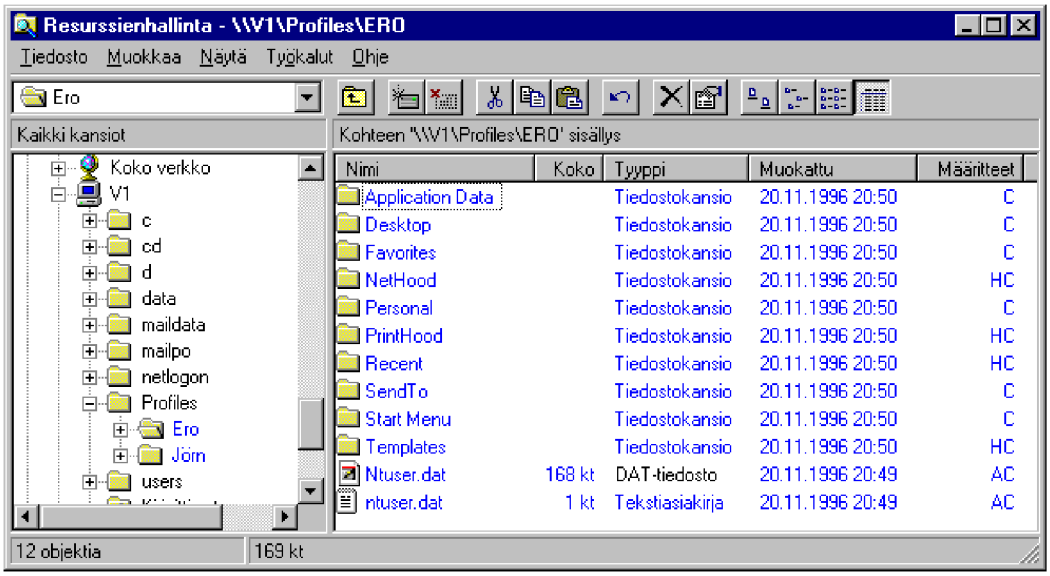
Tässä esimerkissä on ensin valittu useampi käyttäjä ja sitten on määritelty jokaiselle oma profiili **%USERNAME%**-ympäristömuuttujan avulla viittaamaan palvelimella sijaitseviin henkilökohtaisiin profiilihakemistoihin.



Käyttäjänhallinta osaa nimittäin korvata **%USERNAME%**-ympäristömuuttujalla sijainnin käyttäjätunnuksen mukaiseen hakemistoon:



Profiili luodaan ensimmäisen kirjautumisen yhteydessä, tarkkaan ottaen vasta pois kirjautumisen (*Logoff* tai *Logout*) yhteydessä. Käyttäjätunnuksen **ERO** profiilihakemisto näyttää tältä:



Käyttäjän profiili voi myös olla **pakollinen** (*Mandatory*), jolloin käyttäjä ei voi muuttaa profiiliaan. Se tehdään uudelleennimeämällä käyttäjän profiilihakemistossa sijaitseva **NTUser.dat**-tiedosto nimelle **NTUser.man**.

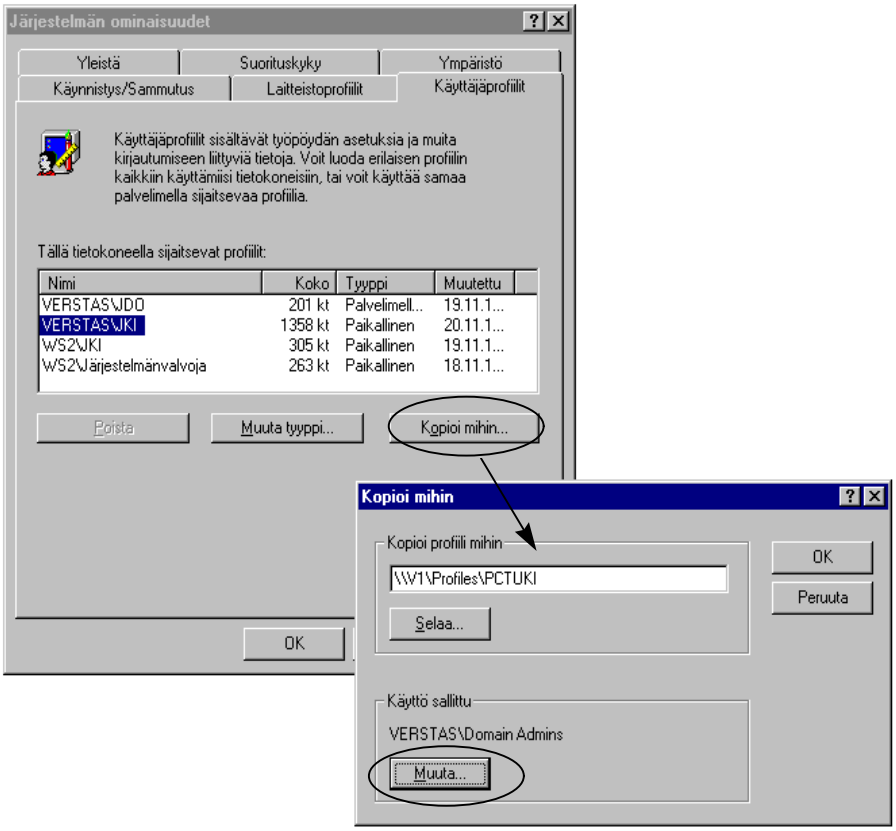
Jos samaa profiilia käyttää useampi käyttäjätunnus, älä määritä yhteistä henkilökohtaista profiilia kaikille tunnuksille, vaan määritä pakollinen profiili kaikille käyttäjille uudelleennimeämällä käyttäjien yhteisen profiilin **NTUser.dat**-tiedosto nimelle **NTUser.man**.

Pakollinen profiili useammalle käyttäjälle tehdään seuraavasti:

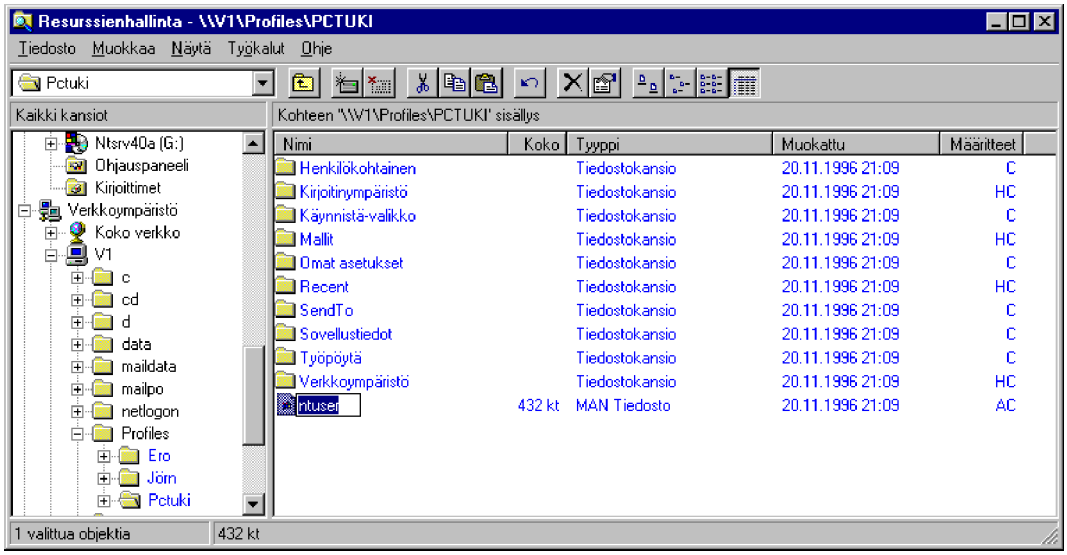
1) Voit ensin kirjautua sopivalla käyttäjätunnuksella NT-työaseman käyttäjäksi

2) Luo **Työpöydälle** ja **Käynnistä** (Start)-painikkeen valikoihin sopiva työskentely-ympäristö

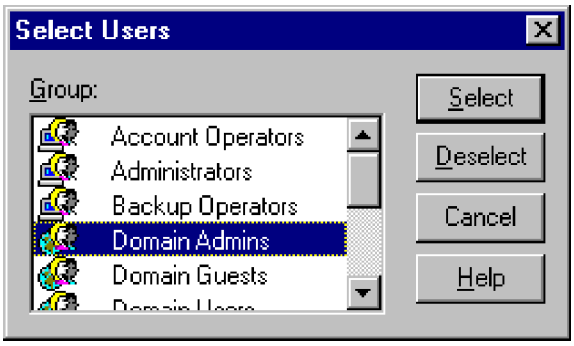
3) Muuta käyttäjän profiilin sijainti **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen **Käyttäjäprofiilit** (User Profiles)-välilehden **Kopioi mihin** (Copy To)-painikkeella viittaamaan palvelimella sijaitsevaan hakemistoon, tässä tapauksessa **\\V1\Profiles\PCTUKI**. Anna myös sopivalle ryhmälle oikeudet profiilin käyttöön **Muuta** (Change)-painikkeella.



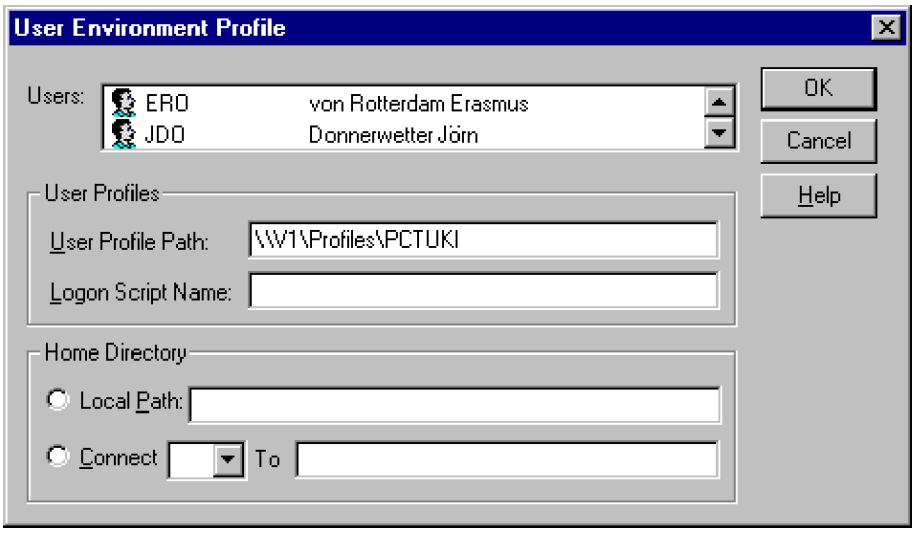
4) Käy tämän jälkeen Resurssienhallinnalla muuttamalla kyseisessä hakemistossa (tässä esimerkin tapauksessa **\\V1\Profiles\PCTUKI)** tiedosto **NTUser.dat** nimelle **NTUser.man**. Tiedostotyyppi muuttuu samalla **MAN-tyyppiseksi**. Tiedostotyypin muutto aiheuttaa sen, että käyttäjä ei voi muuttaa profiiliaan. Tällöin viimeksi profiilia käyttänyt käyttäjä ei muuta (vahingossakaan) profiilin asetuksia.



5) Käynnistä tämän jälkeen **User Manager for Domains** ja valitse profiilia käyttävät käyttäjätunnukset. Voit valita yhden tai käyttäjäryhmän valinnalla **User** | **Select Users**.



6) Valitse **User** | **Properties** tai paina **Enter**, niin voit muuttaa valittujen käyttäjien asetuksia. Muuta profiili viittaamaan hakemistoon, johon edellä tallensit halutun profiilin. Kyseiseen hakemistoon riittää käyttäjille vain lukuoikeus **Read**.

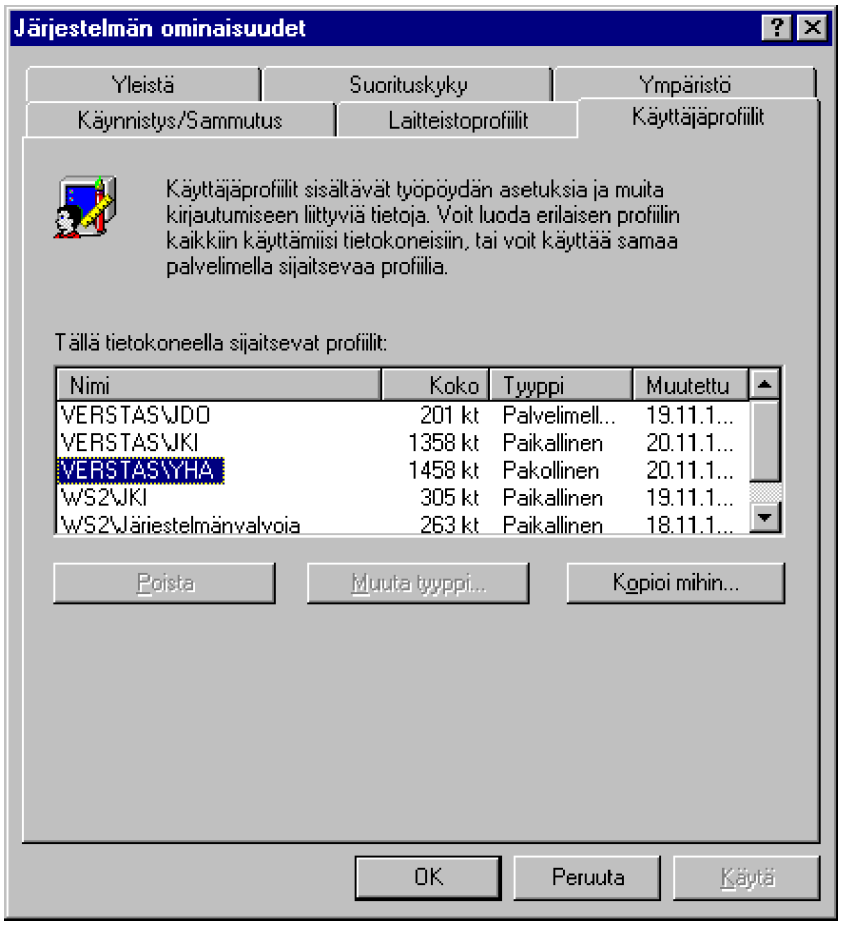


Tällöin käyttäjät eivät voi tallentaa esimerkiksi työpöydän muutoksia

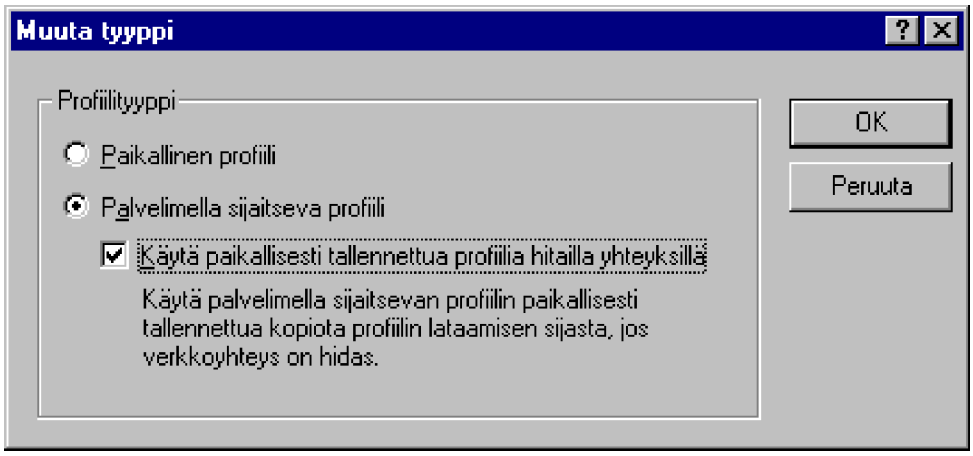
7) Tämän jälkeen valituilla käyttäjillä on yhteinen, pakollinen profiili.

Kun käyttäjä kirjautuu NT-työasemaan, hän saa käyttöönsä palvelimelle tallennetun profiilin.

Voit tarkistaa NT-työasemassa profiilin tyypin **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen **Käyttäjäprofiilit** (User Profiles)-välilehden avulla. Profiilin tulisi olla **Pakollinen** (Mandatory), kuten kuvassa **VERSTAS**-toimialueen **YHA**-käyttäjällä on.



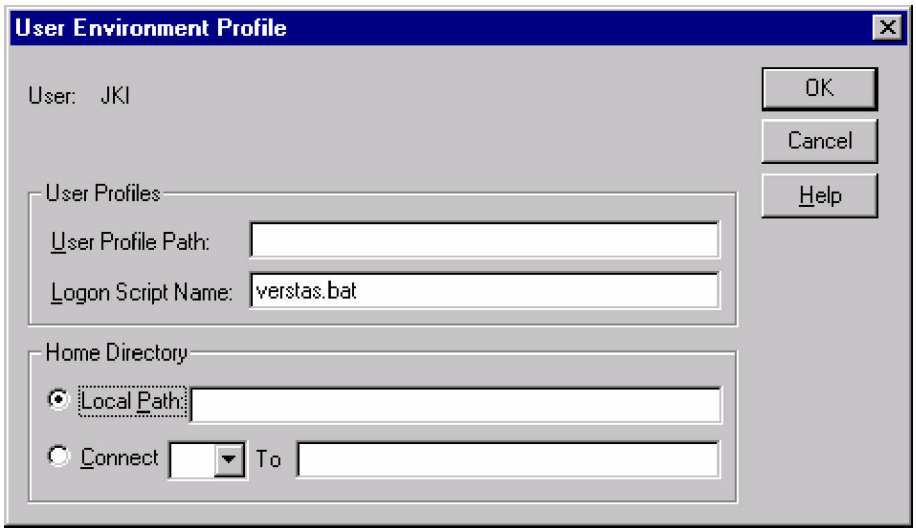
Muuta tyyppi (Change Type) -painikkeella voit tarvittaessa muuttaa profiilin sijaintia. Jos profiili on paikallinen, et tavallisesti voi muuttaa profiilia palvelimella sijaitsevaksi; sen sijaan **Palvelimella sijaitsevan profiilin** (Roaming profile) voit muuttaa **Paikalliseksi** (Local). Vaikka käytössä olisikin **Palvelimella sijaitseva profiili** (Roaming profile), voit sen sijasta määritellä käyttöön paikallisen profiilin käytettäessä hitaita yhteyksiä, esimerkiksi puhelinverkkoyhteyttä.



Tällöin profiilia (jonka koko voi olla useita megatavuja) ei kuitenkaan ladata hitaan yhteyden kautta käyttöön, vaan käytetään paikallista, mikron kiintolevylle tallennettua profiilia.

Kirjauskomentosarja

Jos haluat määrittää kirjauskomentosarjan (kirjauskomentojonon), kirjoita sen tiedostonimi tarkentimineen **Logon Script Name** -ruutuun.



Kirjauskomentosarja (*Logon Script*) (esimerkissä **VERSTAS.BAT**) suoritetaan, kun käyttäjä kirjoittautuu toimialueelle. Sen avulla voit esimerkiksi suorittaa automaattisesti erilaisia rutiineja käyttäjän kirjau-

tumisen yhteydessä. Näitä rutiineja voivat olla virustorjuntaohjelman päivitys, päiväyksen hakeminen palvelimelta, viestien saaminen mikrotuelta jne.

Kirjauskomentosarja on polun **\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS** alihakemistossa. Kirjoita tarvittaessa tiedostonimen eteen kyseisen kirjauskomentosarjan polku, esimerkiksi **BATIT\VERKKO.BAT**.

Palvelin jakaa kyseistä hakemistoa verkkoon nimellä **NETLOGON**. Hakemistoon on kuitenkin vain lukuoikeudet, ja nekin ovat **Everyone**-ryhmällä. Jos et muuta oikeuksia verkon kautta, et pääse verkon kautta tallentamaan kyseistä kirjauskomentojonoa. Toinen tapa on tietysti tallentaa kirjauskomentojono paikallisesti palvelimella hakemistoon **\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS**.

Jos haluat lisätä tietoturvallisuutta, voit määritellä käyttäjäkohtaiseen kirjauskomentosarjaan vain kyseiselle käyttäjälle lukuoikeudet. Jos automatisoit käyttäjien luomisen komentojonojen avulla apuna voit käyttää NT:n **CACLS**-komentoa.

Kirjauskomentosarjat voidaan kopioida PDC:ltä BDC-palvelimille monistuspalvelun avulla (Directory Replicator).

Tiedoston tarkennin (*extension*) rajoittaa käyttäjän työaseman käyttöjärjestelmää seuraavasti:

Työasema:	**Tarkennin:**
MS-DOS	.BAT
Windows 3.1	.BAT
WfW 3.11	.BAT
Windows 95	.BAT
OS/2	.CMD
Windows NT	.CMD tai .BAT

Seuraavaksi esimerkinomainen kirjauskomentosarja NT-työasemaa varten (kirjauskomentosarjassa tulee jättää rivinumerot pois):

```
1 @ECHO OFF
2 ECHO Tervetuloa %USERNAME% toimialueelle %USERDOMAIN% !
3 NET USE X: /D > NUL
4 NET USE X: \\V1\DATA > NUL
5 NET TIME \\V1 /SET /Y
6 START /B NOTEPAD \\V1\INFO\INFO.TXT
```

Rivien selitykset ovat seuraavat:

1 Kaiutus pois käytöstä
2 Tervetuloa - se todennäköisesti vain vilahtaa näytössä
3 Otetaan pois käytöstä mahdollinen X:-levyasema
4 Otetaan X:-asemaksi palvelimen V1 jakama DATA-hakemisto
5 Asetetaan työasemaan palvelimen V1 päiväys ja kellonaika
6 Vaikkapa tukihenkilöiden viimeisimmät vinkit Notepadilla

Useimmissa Microsoftin verkko-ohjelmistoissa saat kotihakemistosi käyttöön komennolla:

NET USE X: /HOME

Windows NT:ssä käytettävissä olevia ympäristömuuttujia ovat:

Ympäristömuuttuja	Merkitys
%COMPUTERNAME%	Tietokoneen nimi
%HOMEDIR%	Kotihakemisto
%HOMEDRIVE%	Kotihakemiston levyasema
%HOMEPATH%	Kotihakemiston hakemisto
%HOMESHARE%	Kotihakemiston UNC-nimi
%OS%	Käyttöjärjestelmä
%PROCESSOR_ARCHITECTURE%	CPU:n tyyppi
%USERDOMAIN%	Käyttäjän toimialue
%USERNAME%	Käyttäjätunnus
%USERPROFILE%	Käyttäjän profiilin hakemisto

Huomaa, että et voi käyttää näitä kuin NT-työasemissa.

Windows 95 ja Työryhmä-Windows 3.11 eivät tue kaikkia e.m. ympäristömuuttujia, mutta edellisessä kirjauskomentojonoesimerkissä vain rivit 2 ja 6 kaipaavat editointia. Kirjauskomentosarjan suoritusta näissä käyttöjärjestelmissä ohjaa tiedosto nimeltä **LMSCRIPT.PIF**. Tarkista, että siinä on asetettu **Sulje ikkuna lopetettaessa** (Close Window On Exit). Tiedosto sijaitsee esimerkiksi **C:\WINDOWS\SYSTEM** -hakemistossa.

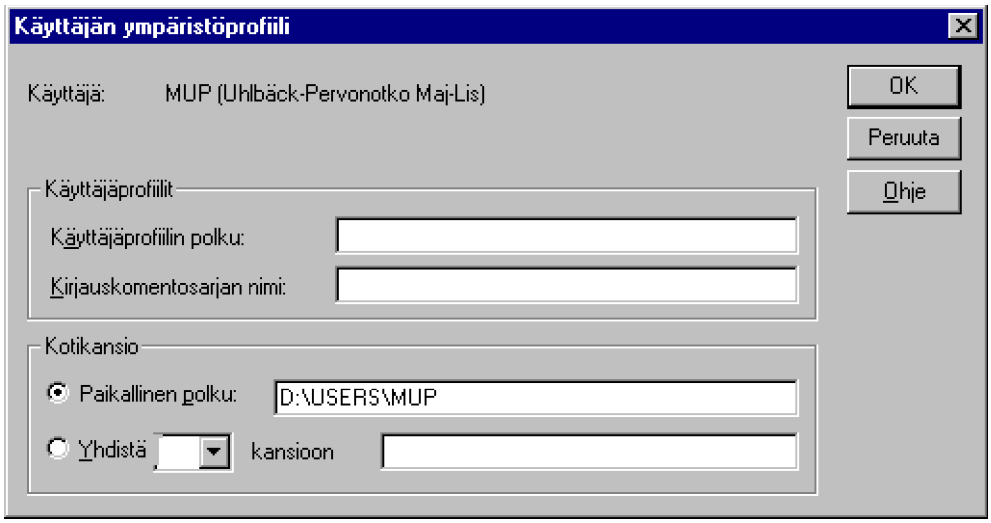
Useamman toimialueen ympäristössä (esimerkiksi *Master Domain*) käyttöön sopiva kirjauskomentosarja:

```
1 @ECHO OFF
2 ECHO Tervetuloa %USERNAME% toimialueelle %USERDOMAIN%
3 NET USE X: /D > NUL
4 IF %USERDOMAIN%==ATK NET USE X: \\A1\DATA > NUL
5 IF %USERDOMAIN%==FISHWARE NET USE X: \\F1\DATA > NUL
6 IF %USERDOMAIN%==LABRA NET USE X: \\L1\DATA > NUL
7 NET USE Y: /D > NUL
8 NET USE Y: \\L1\ASENNUS > NUL
9 NET TIME /DOMAIN:%USERDOMAIN% /SET /Y
10 CALL Y:\UPDATE.BAT
11 START /B NOTEPAD X:\INFO\INFO.TXT
```

Rivien selitykset ovat seuraavat:

1 Kaiutus pois käytöstä
2 Tervetuloa - se todennäköisesti vain vilahtaa näytössä
3 Otetaan pois käytöstä mahdollinen aiemmin kytketty X:-levyasema
4 Jos käyttäjän **toimialue** on **ATK**, otetaan X:-asemaksi palvelimen A1 jakama DATA-hakemisto
5 Jos käyttäjän **toimialue** on **FISHWARE**, otetaan X:-asemaksi palvelimen F1 jakama DATA-hakemisto
6 Jos käyttäjän **toimialue** on **LABRA**, otetaan X:-asemaksi palvelimen L1 jakama DATA-hakemisto
7 Otetaan pois käytöstä mahdollinen aiemmin kytketty Y:-levyasema
8 Otetaan Y:-asemaksi palvelimen L1 jakama Asennus-hakemisto
9 Asetetaan työasemaan oman toimialueen palvelimen päiväys ja kellonaika - tämä edellyttää NT-työasemassa vähintään **Tehokäyttäjien** (Power Users)-ryhmään kuulumista!
10 Ajetaan mahdollinen päivityksiä suorittava komentojono
11 Tukihenkilöiden viimeisimmät vinkit a.o. toimialueelle Notepadilla

Jos haluat määrittää samalla kotikansion (kotihakemiston), voit valita joko **paikallisen polun** käyttäjän Windows NT -työasemassa tai **verkkopolun** palvelimesta.



Kotihakemiston idea on seuraava:

- Tehostettu tietoturvallisuus - NT antaa automaattisesti käyttäjän kotihakemistoon NTFS-levyllä täydet oikeudet vain kyseiselle käyttäjätunnukselle. Lisäksi saavutetaan keskitetyn hallinnan ja valvonnan edut

- Käyttäjä pääsee hakemistoonsa mistä tahansa verkon työasemasta

- Varmistus on helpompaa, koska käyttäjien työtiedostot löytyvät yhdestä hakemistorakenteesta

- Levytilan käyttöä voidaan valvoa - tosin Windows NT 4.0:n mukana ei tule omaa **Quota Manager**-ohjelmaa

- Hakemistot voidaan siirtää toiseen palvelimeen - käyttäjien kannalta tämä tapahtuu läpinäkyvästi - pääkäytäjä muuttaa viittausta kotihakemistoon.

Tee seuraavasti:

- Paikallinen polku valitaan valitsemalla **Paikallinen polku** (Local Path)-ruutu ja kirjoittamalla paikallisen levyaseman tunnuksen ja paikallisen polun, esimerkiksi **D:\USERS\ROLF**. Hakemistopolku alihakemistoineen on myös syytä luoda esimerkiksi **Resurssienhallinnan** (Explorer) avulla! Jos et määritä kotihakemistoa, järjestelmä liittää käyttäjätilin paikalliseen oletusarvona olevaan kotihakemistoon (esimerkiksi paikallisen levyaseman **\USERS\DEFAULT**-hakemistoon, johon NT on asennettu).

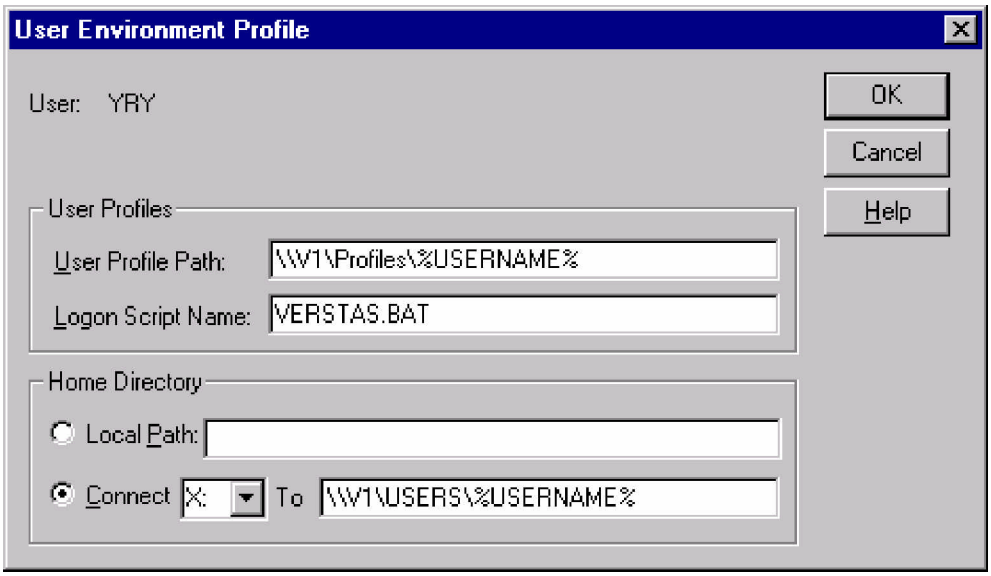
- Verkkopolku valitaan valitsemalla **Yhdistä** (Connect)-ruutu ja määrittämällä aseman tunnus. Valitse sitten **kansioon** (To)-ruutu ja kirjoita verkkopolku. Määritä aseman tunnukseksi esimerkiksi **H:** ja kirjoita koko verkkopolku UNC-nimenä **\\SERVER1\USERS\ROLF**:

  - Jos palvelimen hakemisto **USERS** on jaettu verkkoon NTFS-levyltä, asiat automatisoituvat huomattavasti! Tällöin käyttäjälle luodaan kotihakemisto ja lisäksi NTFS antaa samalla suoraan kyseiselle käyttäjälle hakemistotasolla täydet oikeudet käyttäjän omaan kotihakemistoon!

  - Hallittaessa toimialueen käyttäjätunnuksia on mielestäni syytä **aina** määritellä verkkopolku

  - Kotikansion polun viimeisen alihakemiston voi korvata käyttäjänimellä **%USERNAME%**. Tämä on kätevää, jos on valittu useita käyttäjiä käsiteltäväksi, tai halutaan kopioida mallikäyttäjän asetuksia uusiin käyttäjätunnuksiin.

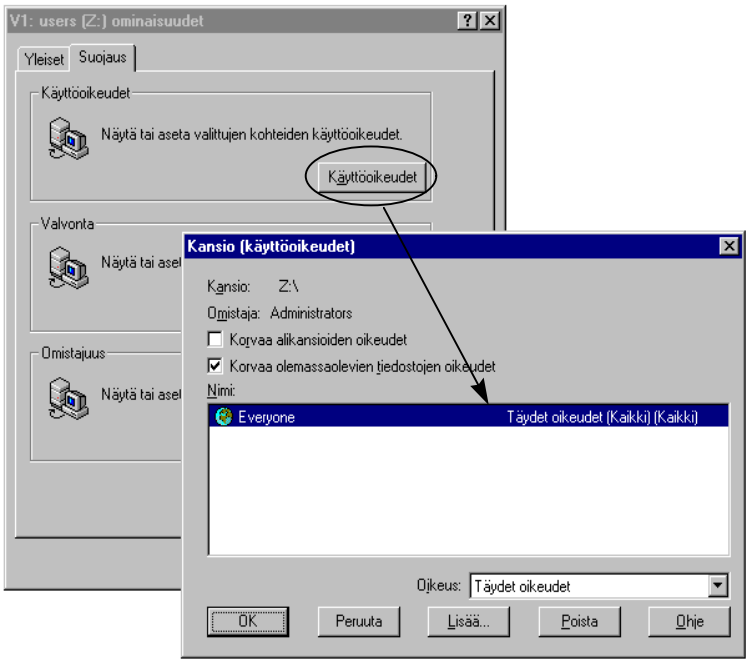
Käyttäjän kotihakemisto luodaan samalla kun käyttäjän muutkin profiilin liittyvät asiat.



Jos **USERS**-hakemisto ei ole jaettu verkkoon, saat seuraavan ilmoituksen, joka kertoo, että hakemisto on luotava käsin:

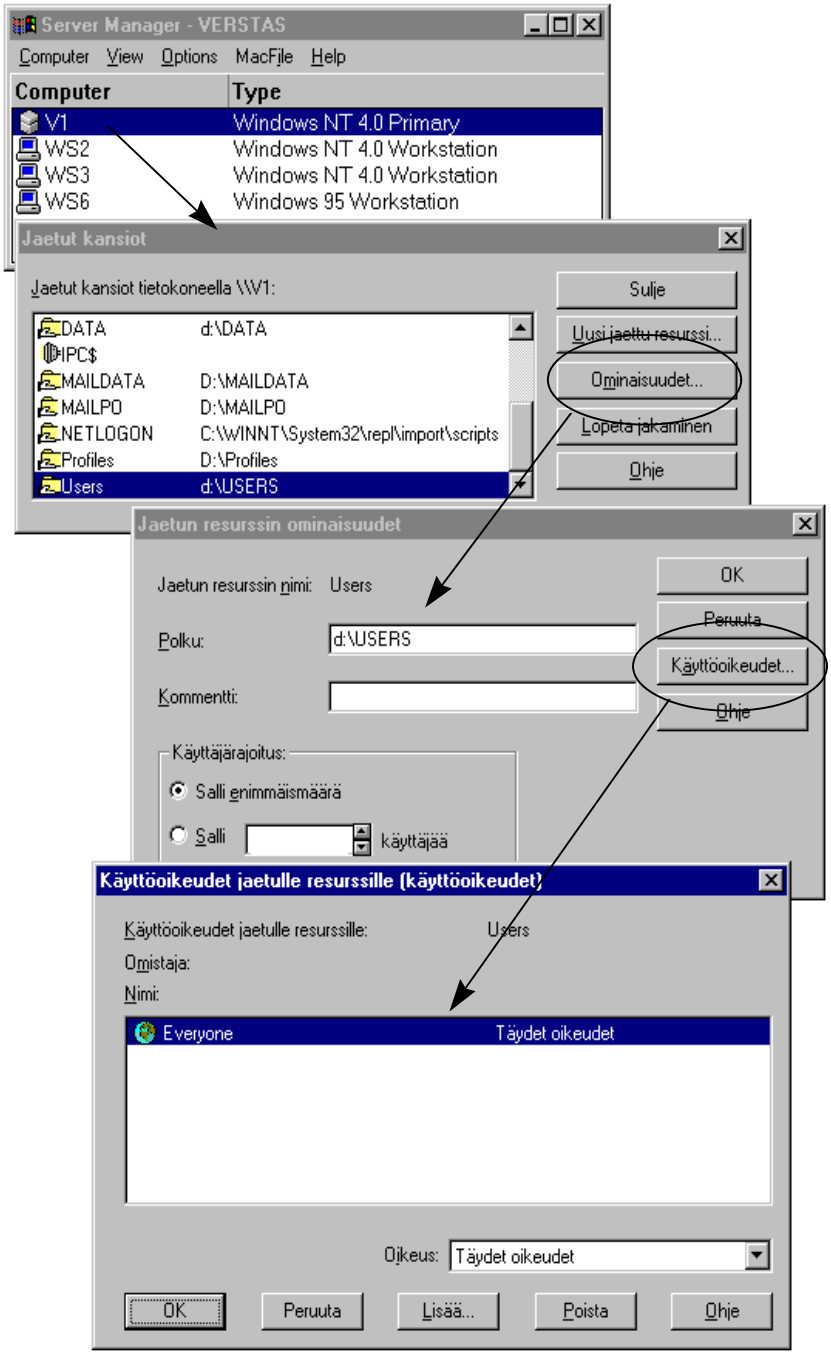
Käyttäjien kotihakemiston juurihakemistoon, esimerkiksi **Users**-hakemistoon, pätevät seuraavat kaksi sääntöä:

1) Sen tulee sijaita NTFS-levyllä ja oletuksena **Everyone**-ryhmällä onhakemistotasolla täydet oikeudet (**Full Control**).



Tätä voi muuttaa niin, että **Administrators**-ryhmällä on **Full Control** ja **Everyone**-ryhmällä on vain **List**-oikeus. List-oikeus tarvitaan, jotta käyttäjät voivat selata kotihakemistonsa. Kotihakemistoissaan käyttäjillä on **Full Control**-oikeus.Voit myös lisätä tietoturvallisuutta antamalla vain tunnetuille käyttäjäryhmille (ts. niille käyttäryhmille, joiden käyttäjien kotihakemistot sijaitsevat kyseisessä hakemistossa) **List**-oikeuden.

2) Se on oletuksena jaettu palvelimelta verkkoon **Everyone**-ryhmälle täysillä oikeuksilla **Full Control**. Tämän voit tarkistaa palvelimella valitsemalla a.o. hakemiston pikavalikosta **Sharing** tai **Server Managerissa Computer** -valikosta **Shared Directories** sekä **Properties**.

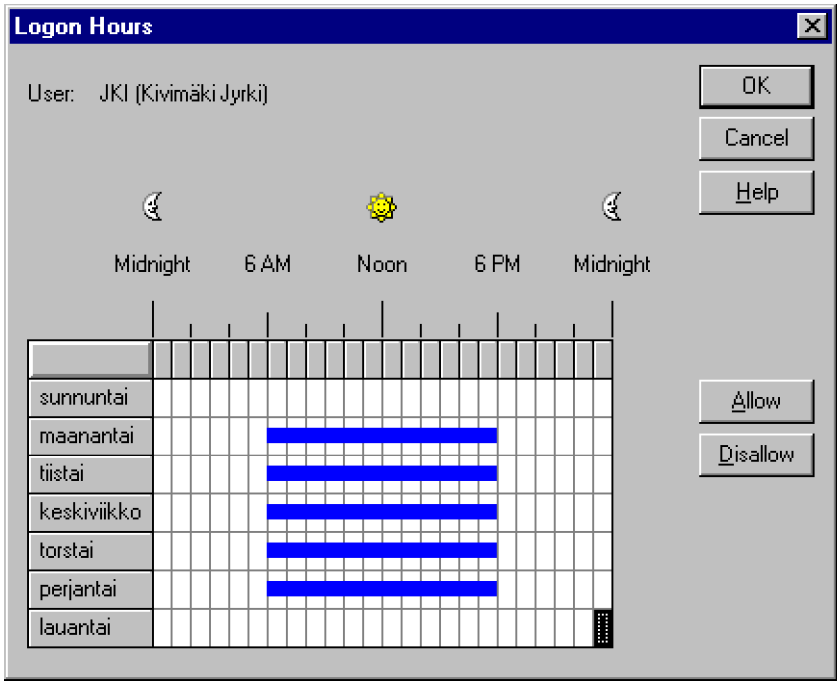


Tätä voi muuttaa niin, että **vain** tunnetuilla käyttäjäryhmillä ja **Administrators**-ryhmällä on **Full Control**-oikeus.

Kirjautumisajat

Logon Hours-valintaikkunan avulla rajoitetaan aikoja, jolloin käyttäjä voi muodostaa yhteyden palvelimeen.

Oletusarvona on, että käyttäjä voi muodostaa yhteyden palvelimeen aina halutessaan, mutta kirjautumisaikoja voidaan myös rajoittaa. Rajoitus ei vaikuta työaseman käyttömahdollisuuksiin.



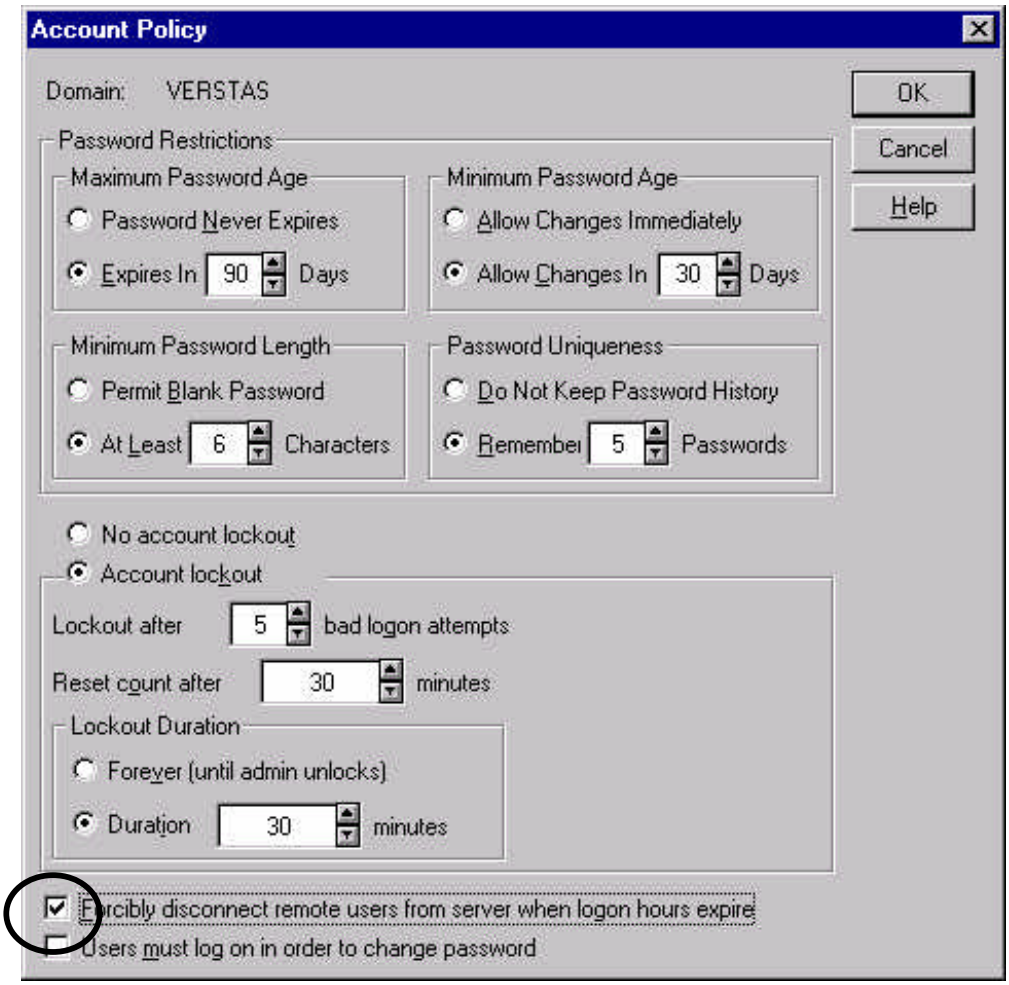
JKI:lle on mahdollista työskentely toimialueella vain maanantaista perjantaihin klo 06-18.

Valitse haluamasi ajat; valitse yksi tunti napauttamalla kyseisen tunnin ruutua. Valitse useita tunteja napauttamalla ensimmäistä valitsemaasi tuntia ja merkitsemällä loput rivit ja sarakkeet hiirellä vetämällä. Voit valita koko päivän napauttamalla kyseisen päivän nimeä vasemmassa sarakkeessa; jos haluat valita yhden tunnin jokaisena päivänä, napsauta sarakkeen ylimmäistä ruutua. Valitse koko viikko napauttamalla vasemmassa yläkulmassa olevaa ruutua.

Valitsemalla **Allow**-painikkeen annat oikeuden työskennellä toimialueella kyseiseen aikaan ja estää työskentely **Disallow**-painikkeella. Paina lopuksi **OK**.

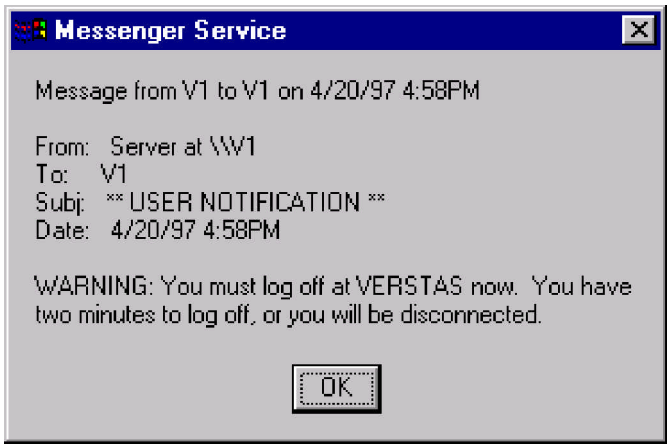
Jos käyttäjä yrittää kirjautua toimialueelle aikaan, joka ei ole sallittu, kirjautuminen ei onnistu ja siitä tulee huomautus. Windows NT -työasemassa huomautus näyttää tältä:

Valitsemalla User Manager for Domainsissa **Policies** | **Account** voit valita käyttöön etäkäyttäjien pakottamisen palvelimelta, kun kirjautumisaika on päättynyt valinnalla **Forcibly disconnect remote users from server when logon hours expire**.

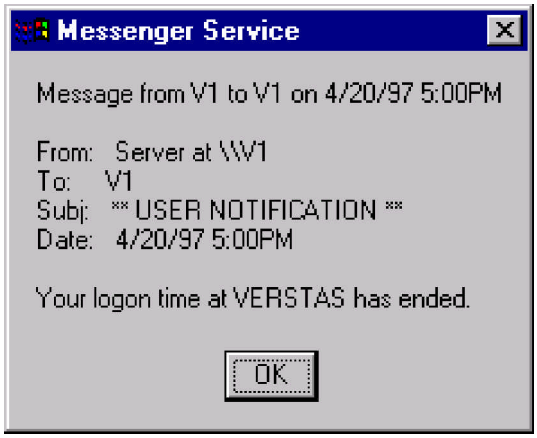


Tällöin käyttäjä saa ennen kirjautumisajan päättymistä työasemaansa ilmoituksen:

Sitten kun alkaa tulla todella kiire, siitäkin huomataan muistuttaa:



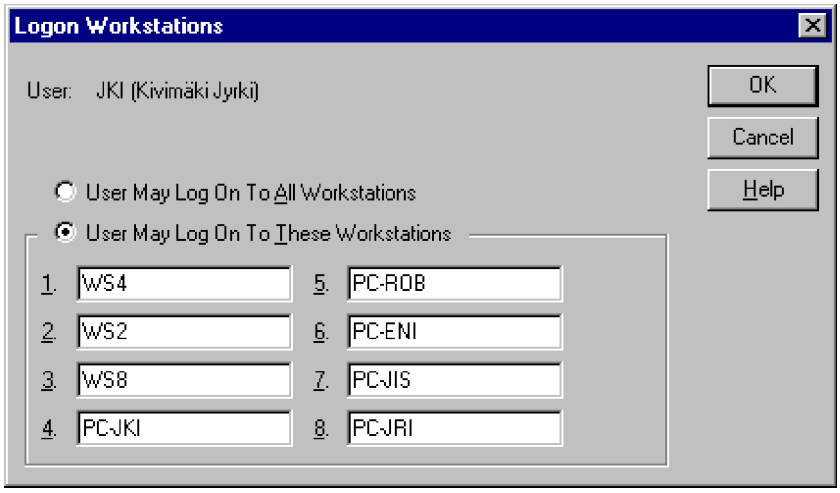
Kun kirjautumisaika on päättynyt, siitä tulee vielä huomautus:



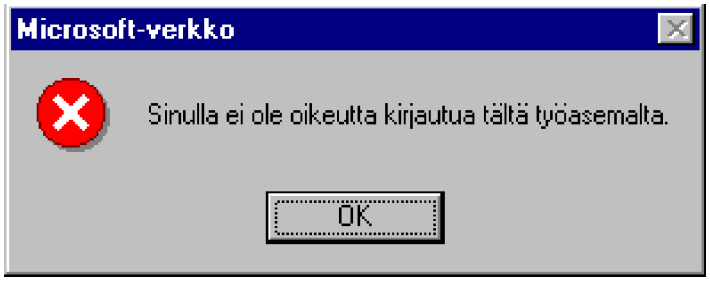
Kirjautumistyöasemat

Logon To-painikkeella asetetaan ne NT-työasemat (tai NT-palvelimet), joista käyttäjä saa kirjoittautua toimialueelle. Asetus koskee myös Windows NT -työasemia.

Anna työasemien nimet 1 - 8 ja valitse **User May Log On To These Workstations** tai salli käyttäjän kirjoittautua mistä tahansa työasemasta valitsemalla **User May Log On To All Workstations**.

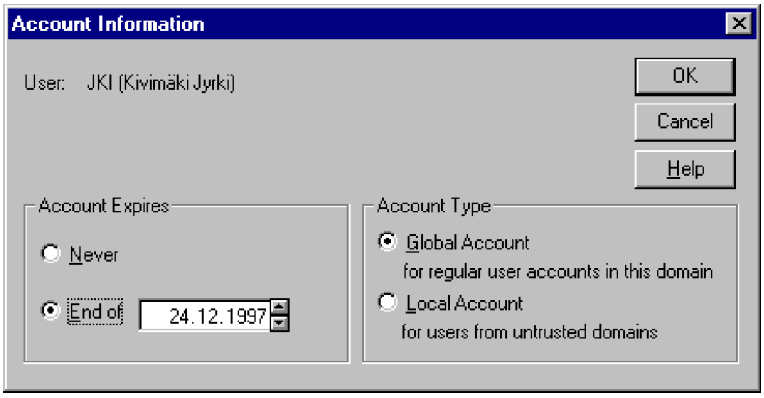


Asetus toimii Windows NT -työasemien lisäksi myös Windows 95 -työasemissa:



Käyttäjätunnuksen vanheneminen

Account-painikkeella voidaan asettaa käyttäjätunnuksen vanheneminen: vaihtoehdot ovat ei koskaan valitsemalla **Never** ja tietyn ajan jälkeen **End of**, minkä jälkeen käyttäjätunnusta ei voi käyttää.

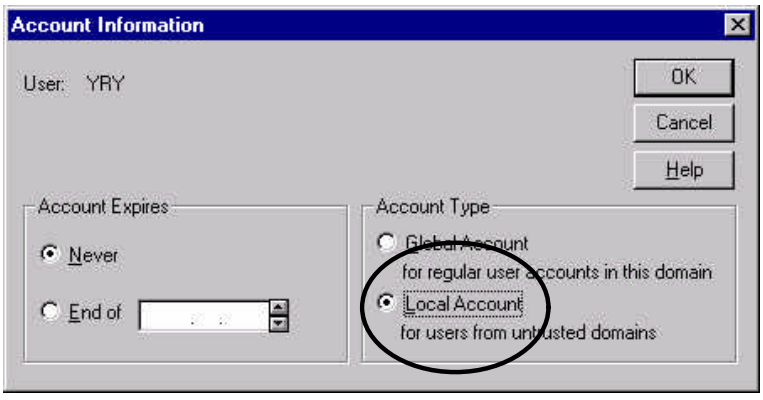


Pääkäyttäjätason (Administrator) käyttäjätunnusten ei tulisi **koskaan** vanhentua!

Käyttäjätunnuksen tyyppi

Account-painikkeella voidaan asettaa käyttäjätunnuksen tyyppi. Käyttäjätunnus voi olla **yleinen** (Global Account), mikä kannattaa normaalisti valita.

Toinen vaihtoehto on **paikallinen** (Local Account); käyttäjätunnus ei näy luottosuhteiden yli, jolloin sama käyttäjätunnus voidaan määritellä myös niihin toimialueisiin, joihin ei (toistaiseksi) ole luottosuhdetta.



Paikallinen (Local Account) käyttäjätunnus ei myöskään näy kyseisen toimialueen Windows NT -työasemiin!

Paikallisen käyttäjätunnuksen hyöty voi olla siinä, että toimialueista, joista ei kyseiseen toimialueeseen ole luottosuhdetta, voidaan ottaa kyseisen toimialueen resursseja käyttöön antamalla kyseisen toimialueen paikallinen käyttäjätunnus:

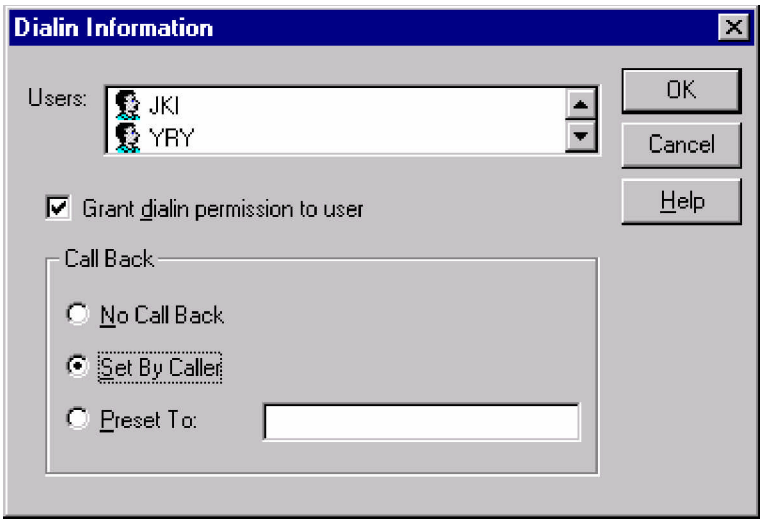
- Levyaseman käyttöönotossa **Yhdistä nimellä** (Connect As)
- Komentorivillä **NET USE /USER:toimialue\käyttäjätunnus**-komennolla.

Puhelinyhteys

Dialin tarkoittaa **etäkäyttöyhteyttä** (RAS, Remote Access Service) Windows NT -työasemaan tai -palvelimeen. Asetuksista riippuen käyttäjälle voidaan sallia myös yhteys lähiverkkoon, johon Windows NT -työasema tai -palvelin on liitetty.

Etäkäyttötyöasema voi olla esimerkiksi Työryhmä-Windows-, Windows 95- tai Windows NT -palvelin/työasema. Etäkäyttöyhteyksiä työasemasta palvelimeen voidaan muodostaa yleisten puhelinlinjojen, X.25-verkkojen tai ISDN-yhteyksien kautta. Etäkäyttöpalvelun avulla etätyöasemat voivat käyttää verkkoa läpinäkyvästi kuin ne olisivat kytkettyinä suoraan verkkoon.

Jotta käyttäjä voi kytkeytyä etäkäyttöyhteyden kautta Windows NT -palvelimeen tai -työasemaan, käyttäjällä tulee olla etäkäyttöoikeudet. Ne annetaan erikseen käyttäjäkohtaisesti **Dialin**-painikkeen avulla. Voit myös valita useamman käyttäjän kerrallaan ja antaa kaikille valituille samalla kertaa etäkäyttöoikeudet, kuten kuvassa on tehty:



Oikeus annetaan rastittamalla ruutu **Grant dialin permission to user**. Kohta **Callback** määrittää, miten takaisinsoiton suhteen tehdään:

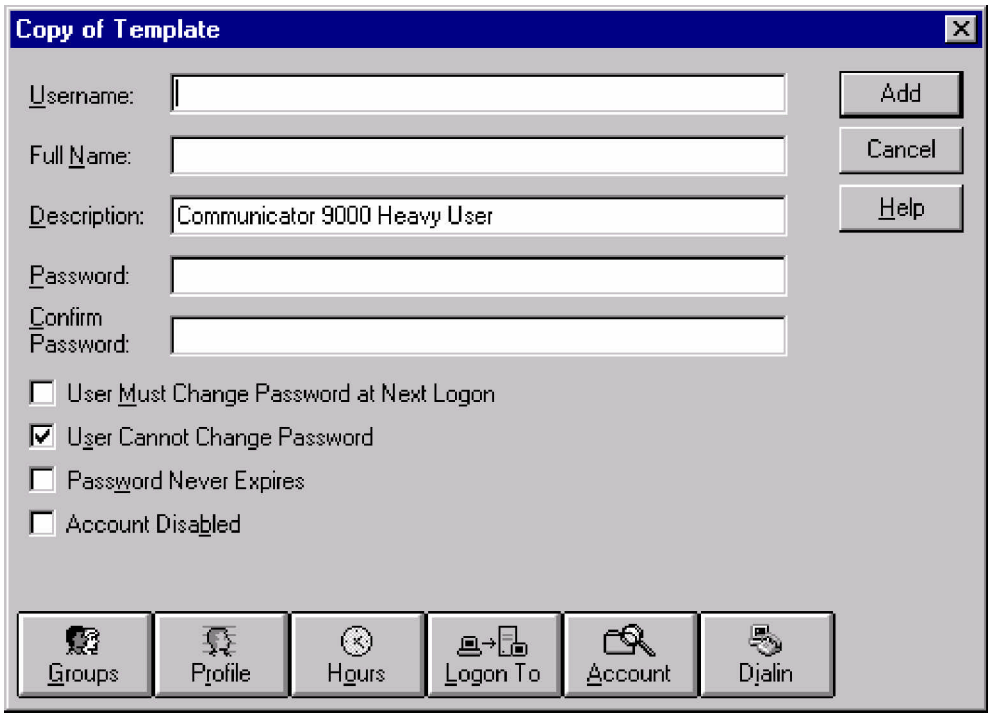
- **No Call Back** ei mahdollista takaisinsoittoa laisinkaan
- **Set By Caller** mahdollistaa yhteyden muodostusvaiheessa takaisinsoiton käyttäjän erikseen antamaan numeroon
- **Preset to** soittaa aina annettuun numeroon ja on tietoturvan kannalta luotettavin vaihtoehto.

Käyttäjätunnusten kopioiminen

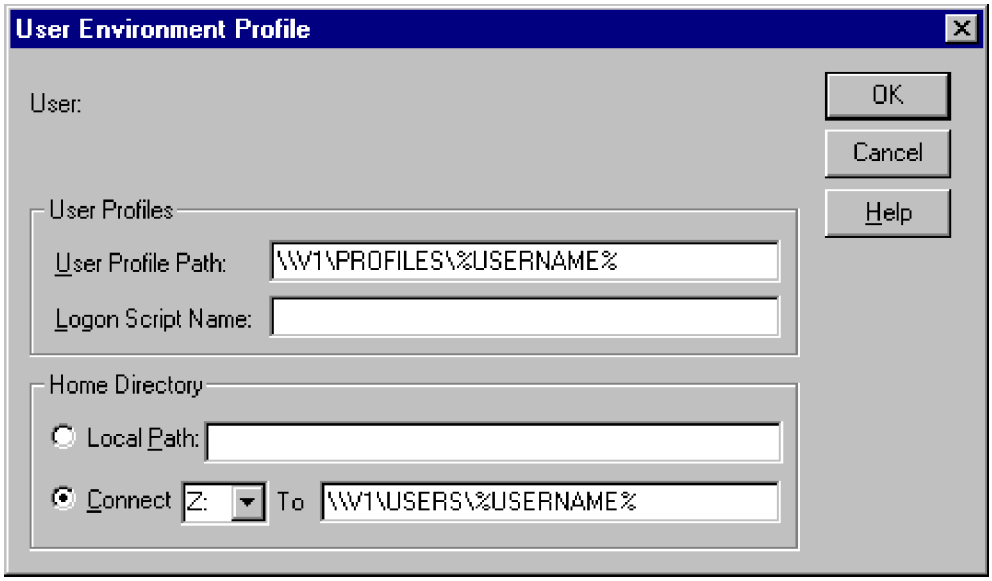
Valmiin käyttäjätunnuksen kopioiminen on nopeampaa ja vaivattomampaa kuin uuden käyttäjätunnuksen luominen. Kopioimisessa on myös se etu, että ryhmäjäsenyydet kopioituvat uuteen tiliin, ja jos profiiliasetukset on asetettu **%USERNAME%**-ympäristömuuttujan avulla, myös ne muuttuvat oikein.

Valitse ensin haluamasi käyttäjätunnus ja valitse **User** | **Copy** tai paina **F8**. Anna uusi käyttäjätunnus ja muut muutettavat asetukset, kuten salasana. Valitse lopuksi **Add**-painike.

Voit tehdä vaikkapa **Template**-nimisen käyttäjätunnuksen, johon asetat kaikki tavalliset käyttäjän asetukset ja käytät tätä käyttäjätunnusta pohjana luodessasi uusia käyttäjätunnuksia.



Ainoastaan käyttäjätunnus, käyttäjän nimi ja salasana ei kopioidu.

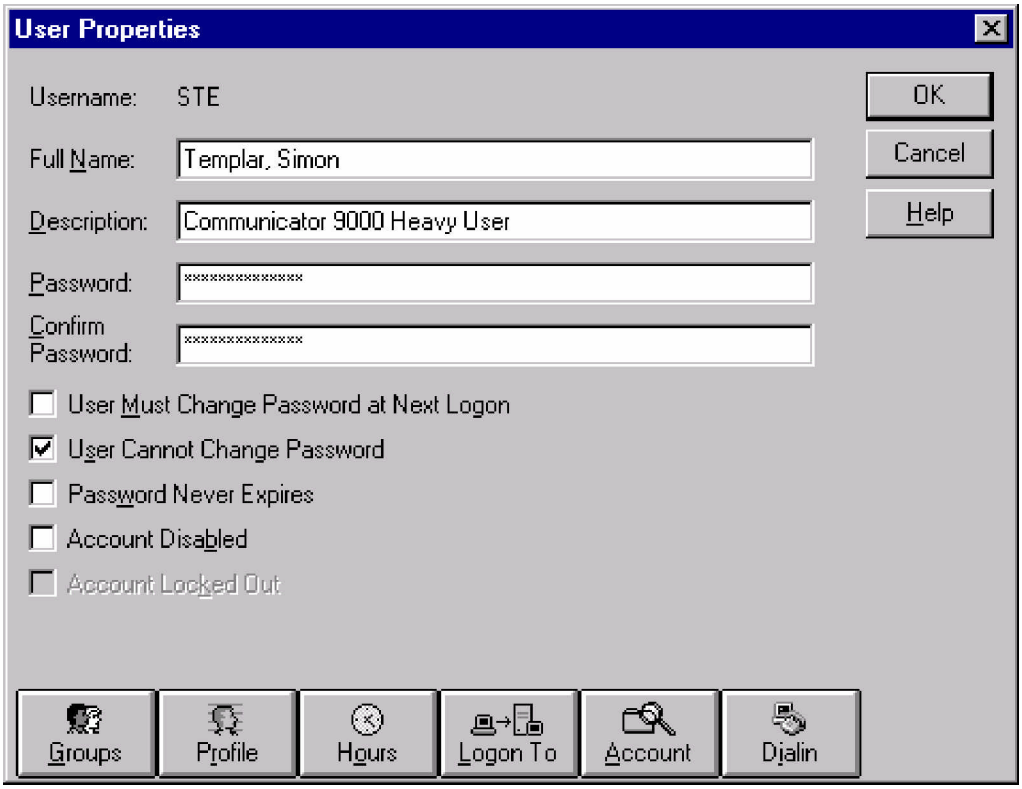


Esimerkki **%USERNAME%**-ympäristömuuttujan käytöstä **Template**-käyttäjän profiilissa:

Käyttäjätunnuksen asetusten muuttaminen

Käyttäjätunnuksen asetusten muuttaminen onnistuu kaksoisnapauttamalla käyttäjätunnuksen päälle tai valitsemalla käyttäjätunnus valitsemalla **User** | **Properties** tai painamalla **Enter**.

Anna uudet asetukset ja paina lopuksi **Close**.



Useiden käyttäjätunnusten asetusten muuttaminen

Kahden tai useamman käyttäjätunnuksen asetusten muuttaminen samanaikaisesti tehdään seuraavasti:

1) Valitse haluamasi käyttäjätunnukset; voit käyttää **Vaihto**- ja **Ctrl**-näppäimiä. Voit valita ensimmäisen käyttäjätunnuksen, painaa **Vaihtonäppäintä** ja **End**-näppäintä, niin viimeinenkin käyttäjä tulee valittua

2) Valitse **User** | **Properties**

3) Anna kuvaus **Description**-kohtaan:

- Jos kaikilla valituilla käyttäjätunnuksilla on samanlainen kuvaus, teksti näkyy kuvausruudussa
- Jos tunnuksilla on erilaisia kuvauksia, ruutu on tyhjä

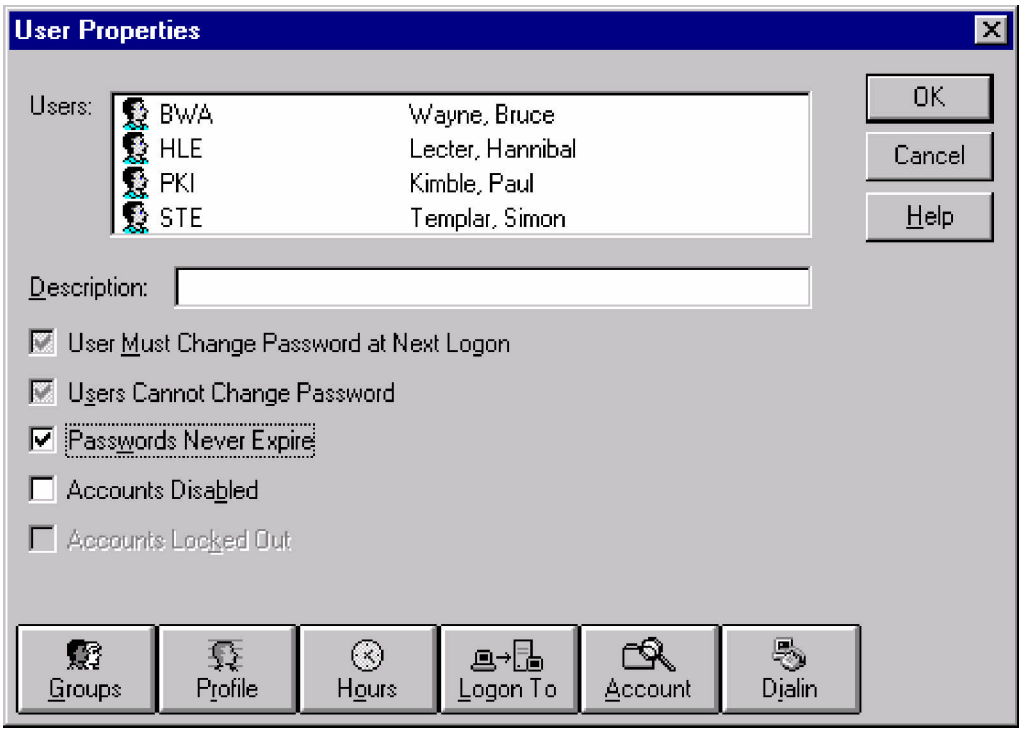
Valitse halutut vaihtoehdot:

- Jos vaihtoehdon asetus on sama kaikilla käyttäjätunnuksilla kyseinen asetus näkyy valintaruudussa (ruutu on tyhjä tai asetus on valittu)
- Jos eri käyttäjätunnusten asetukset poikkeavat toisistaan, valintaruutu on harmaa

Valitse haluamasi painike ja tee tarvittavat määritykset valintaikkunassa

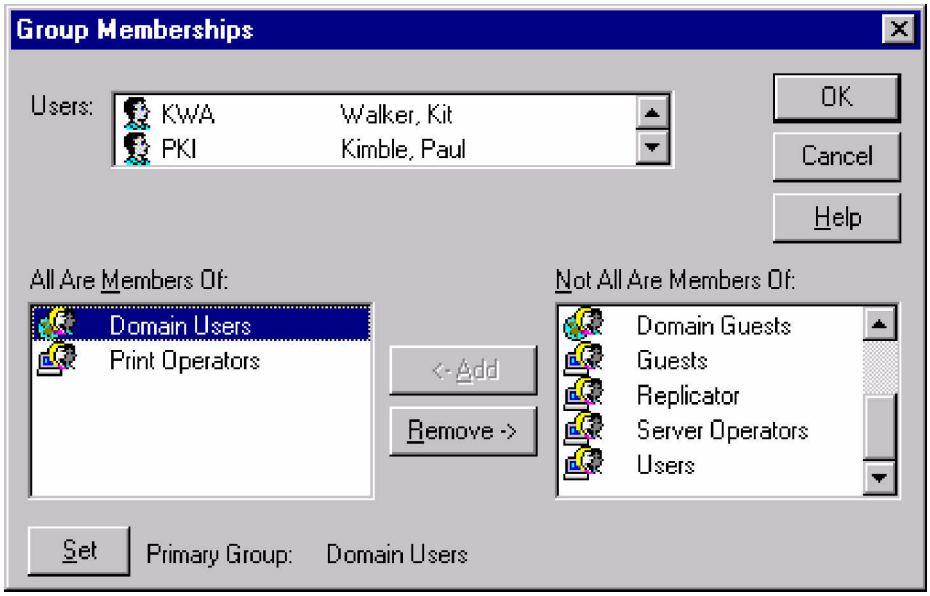
4) Valitse lopuksi **OK**.

Muutokset tulevat voimaan kaikissa valituissa käyttäjätunnuksissa.



Monien käyttäjätunnusten ryhmäjäsenyyksien hallinta

Kun olet valinnut käyttäjätunnukset, voit lisätä ne kerralla **Group Memberships**-valintaikkunan avulla toimialueen ryhmiin. Voit myös poistaa käyttäjätilejä ryhmistä aivan kuten yksittäisen käyttäjänkin kohdalla.

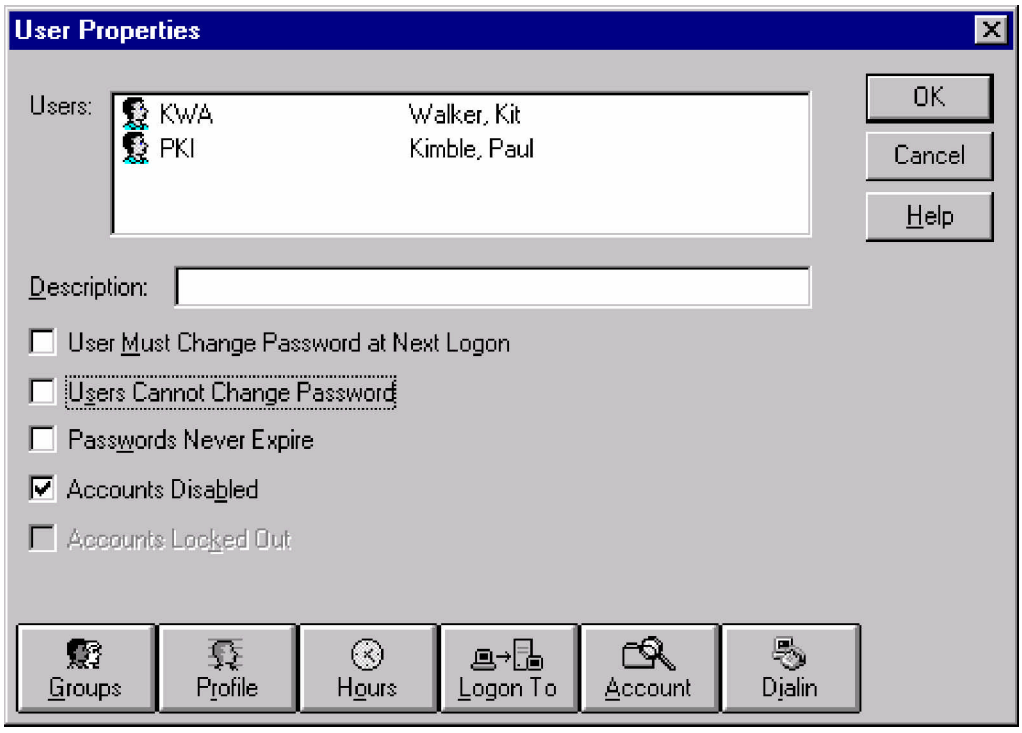


Huomaa, että voit valita samalla kaikille valituille käyttäjille halutun ensisijaisen ryhmän (**Primary Group**)!

Käyttäjätunnusten poistaminen käytöstä

Käytöstä poistettu (*disabled*) käyttäjätunnus näkyy User Manager for Domainsin ikkunan luettelossa, mutta sillä ei voi kirjautua järjestelmään. Käytöstä poistetut tunnukset voidaan ottaa käyttöön milloin tahansa.

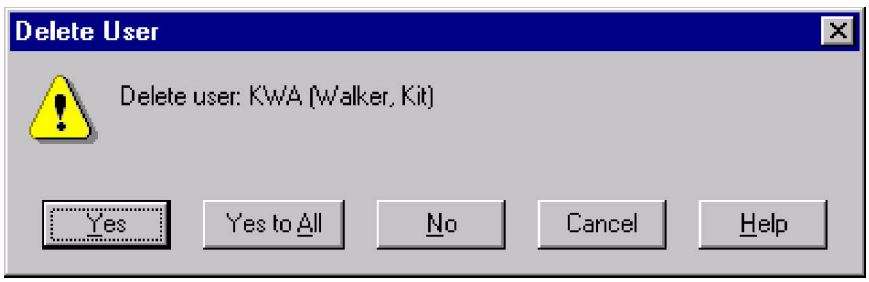
Järjestelmään kuuluvaa **Administrator**-tunnusta ei voi poistaa käytöstä. Valitse yksi tai useampi käyttäjätunnus ja valitse **User** | **Properties**. Estä kirjautuminen valitsemalla **Account Disabled**. Salli käyttö poistamalla vaihtoehdon valinta ja valitsemalla **OK**.



Käyttäjätunnusten poistaminen

Voit poistaa käyttäjätunnuksen valitsemalla yhden tai useamman käyttäjätunnus ja valitsemalla **User** | **Delete** tai painamalla **Delete**-näppäintä. Saat huomautuksen poistosta - valitse **OK,** jos haluat jatkaa:

Voit valita, poistatko kaikki vai yhden valitun käyttäjän kerrallaan:



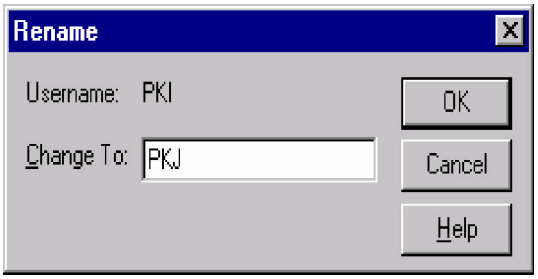
Et voi poistaa asennusvaiheessa luotuja käyttäjätunnuksia: **Administrator** etkä **Guest** - sen sijaan voit poistaa ne väliaikaisesti käytöstä (*disabled*) tai uudelleennimetä (*rename*)!

Detaljina mainittakoon, että et voi myöskään poistaa omaa käyttäjätunnustasi:

Poistettua käyttäjätunnusta ei saa takaisin; jos haluat palauttaa tunnuksen, se on luotava oikeuksineen alusta alkaen uudelleen! Poistaminen poistaa kaikki käyttäjään liittyneet asetukset!

Käyttäjätunnusten nimeäminen uudelleen

Voit nimetä uudelleen yhden käyttäjätunnuksen kerrallaan valitsemalla **User |Rename**.



Käyttäjätunnuksen uudelleenimeäminen ei muuta mitään käyttäjän oikeuksia eikä ryhmäjäsenyyksiä!

Esimerkiksi jos jonkun käyttäjän tilalle tulee toinen henkilö, voit helposti uudelleennimetä poistuneen henkilön käyttäjätunnuksen uudelle henkilölle. Tällöin oikeudet resursseihin säilyvät ennallaan.

Paikallisten ryhmien hallinta

Paikalliset ja yleiset ryhmät ovat Windows NT -ympäristön käyttäjienhallinnan ehkä hankalin asia.

Windows NT:n toimialueen käyttäjätietokannassa on kahdenlaisia ryhmiä:

- **Paikallisia ryhmiä** (*Local Group*) joihin voi kuulua jäsenenä **paikallisia käyttäjiä** sekä **yleisiä ryhmiä** (*Global Group*), mutta **ei** toisia paikallisia ryhmiä. Yleinen ryhmä voi olla oman toimialueen yleinen ryhmä tai luottosuhteen yli **toisen toimialueen** yleinen ryhmä

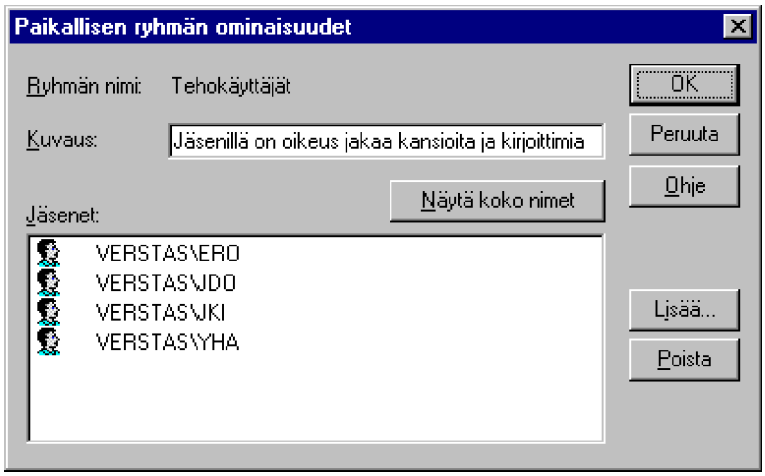
- **Yleisiä ryhmiä** (*Global Group*), joihin voi kuulua jäsenenä **vain toimialueen yleisiä käyttäjiä**.

NT-työaseman **Käyttäjien hallinta** (User Manager) ei ymmärrä eikä pysty luomaan muita kuin **kyseisen NT-työaseman paikallisia ryhmiä**; tällöin ryhmät ja käyttäjät ovat käsiteltävissä ja käytettävissä vain NT-työasemassa paikallisesti. Koska voit käsitellä myös suomenkielisessä Windows NT 4.0-työasemassa näitä käytäntöjä, esittelen myös suomenkieliset komennot.

Jos työasema on liittynyt toimialueeseen, **Käyttäjien hallinnalla** (User Manager) voidaan lisätä työaseman paikallisiin ryhmiin kuitenkin myös **toimialueen yleisiä ryhmiä** ja **yleisiä käyttäjiä**, mutta niitä ei voida luoda eikä muokata. Myöskään **toimialueen paikallisia käyttäjiä** tai **paikallisia ryhmiä** ei voida lisätä työaseman käyttäjäryhmiin tai käyttäjiksi.

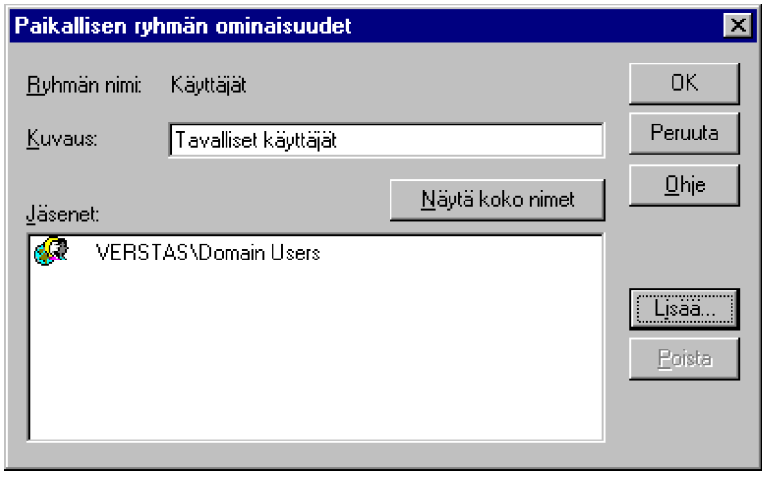
Paikallisia ryhmiä työasemassa ovat mm. **Käyttäjät** (Users) peruskäyttäjille, **Tehokäyttäjät** (Power Users) tehokäyttäjille ja **Järjestelmänvalvojat** (Administrators) työaseman valvojille hallintakäyttöä varten.

Tässä esimerkissä **Käyttäjien hallinta** (User Manager) näyttää tässä työasemassa paikallisen ryhmän **Tehokäyttäjät** (Power Users) jäseniksi vain **toimialueen yleisiä käyttäjätunnuksia**:



Käyttäjäryhmät, jotka alkavat etuliitteellä **Domain...** ovat **aina** toimialueella määriteltyjä käyttäjäryhmiä.

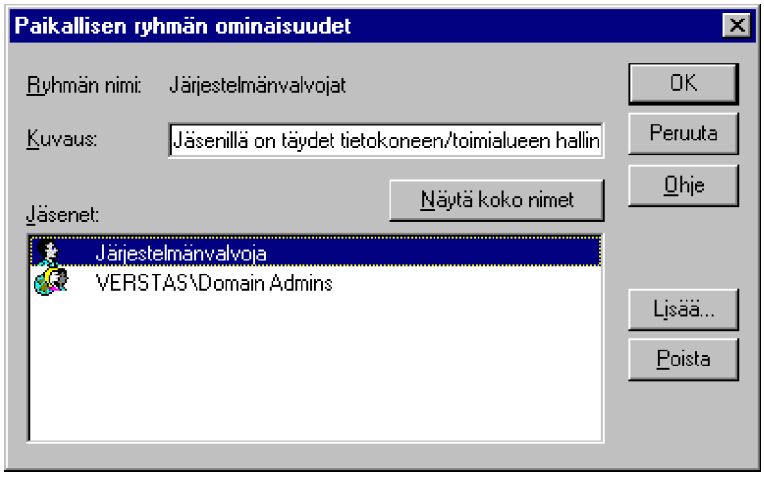
Toimialueen yleinen käyttäjien ryhmä **Domain Users** lisätään **automaattisesti** työaseman paikalliseen **Käyttäjät** (Users)-ryhmään, kun työasema lisätään toimialueelle; tällöin työaseman paikalliseen käyttäjäryhmään kuuluvat automaattisesti myös kaikki toimialueen käyttäjätunnukset:



Tässä tapauksessa toimialueen nimi on **VERSTAS** ja ryhmän nimi on **Domain Users**.

Vastaavasti toimialueen yleinen järjestelmänvalvojien ryhmä **Domain Admins** lisätään automaattisesti työaseman paikalliseen **Järjestelmänvalvojat** (Administrators)-ryhmään, kun työasema lisätään toimialueelle.

Tällöin työaseman paikalliseen järjestelmänvalvojien ryhmään kuuluvat automaattisesti myös kaikki toimialueen järjestelmänvalvojien käyttäjätunnukset. Oletuksena ryhmään kuuluu joka tapauksessa myös **työaseman paikallinen Järjestelmänvalvoja** (Administrator)-käyttäjätunnus.



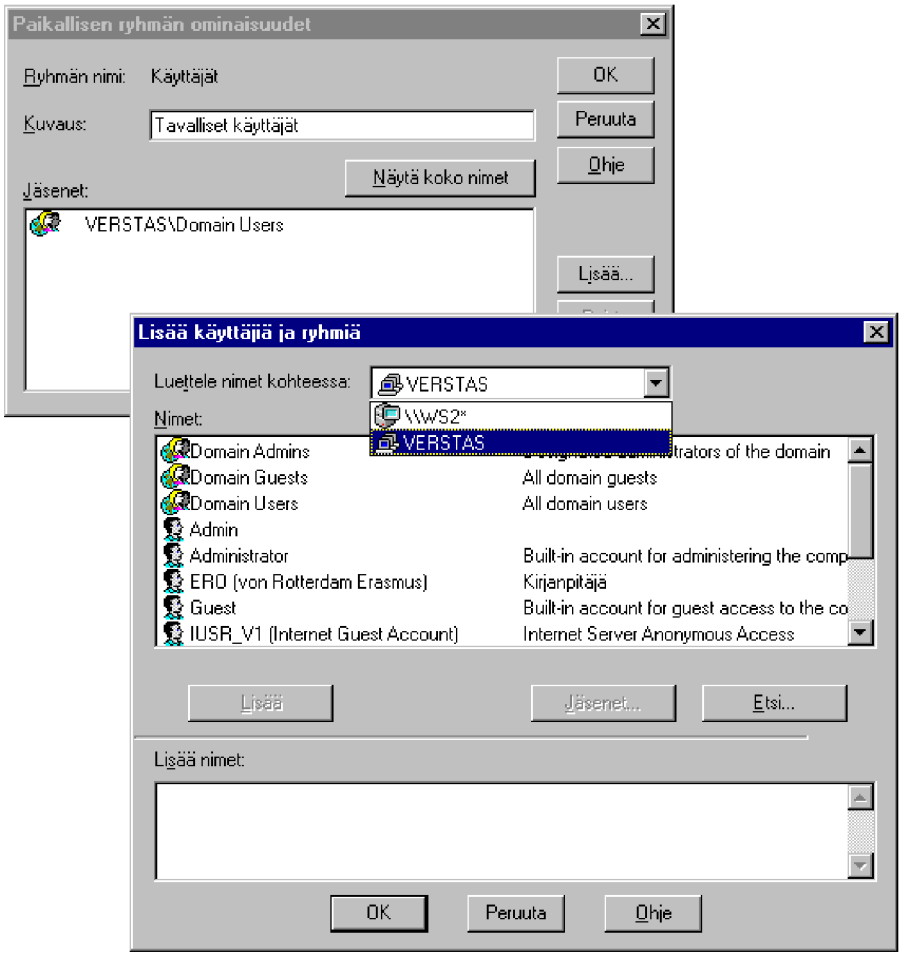
Tässä tapauksessa toimialueen nimi on **VERSTAS** ja ryhmän nimi on **Domain Admins**.

Edellä mainitut ryhmäjäsenyydet helpottavat hallintaa huomattavasti, koska nyt riittää käyttäjätunnuksien määrittely vain toimialueella! Käyttäjä, joka kuuluu toimialueen **Domain Users**-ryhmään kuuluu toimialueen NT-työasemissa oletuksena NT-työaseman paikalliseen **Users**-ryhmään.

Jos työasema on liitetty toimialueelle, tämä ryhmien lisääminen on siis jo tehty automaattisesti.

Toimialueelle liitetyssä NT-työasemassa voit valita, lisätäänkö käyttäjiä paikalliseen ryhmään työaseman omasta käyttäjätietokannasta (WS2) vai toimialueelta (VERSTAS).

Jos toimialueelta olisi **luottosuhteita** toisiin toimialueisiin, niidenkin nimet näkyisivät luettelossa, ja näiden toimialueiden yleiset käyttäjätunnukset ja yleiset käyttäjäryhmät olisivat myös lisättävissä NT-työaseman paikalliseen ryhmään.

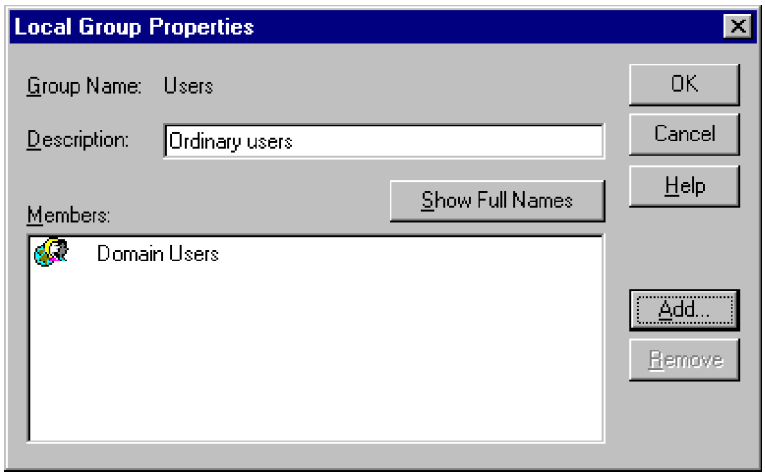


User Manager for Domains sen sijaan hallitsee paitsi paikalliset, myös yleiset ryhmät (Global Groups) ja yleiset käyttäjätunnukset. Yleinen ryhmä ja yleinen käyttäjä näkyvät toimialueeseen kuuluvassa NT-työasemassa ja luottosuhteen yli toisessakin toimialueessa; **toimialueen paikallinen käyttäjä** tai **paikallinen ryhmä** sen sijaan ei näy, eikä sitä voida lisätä toisen toimialueen käyttäjäryhmiin.

Toimialueen paikallisia ryhmiä ovat mm. **Users** peruskäyttäjille ja **Administrators** pääkäyttäjille/järjestelmänvalvojille toimialueen paikallista hallintakäyttöä varten.

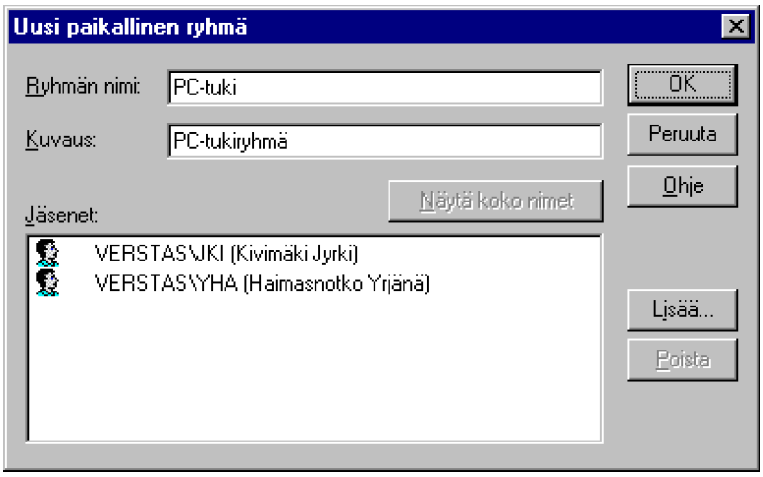
Toimialueen yleisiä ryhmiä ovat mm. **Domain Users** peruskäyttäjille ja **Domain Admins** pääkäyttäjille/järjestelmänvalvojille hallintakäyttöä varten.

User Manager for Domains ja yleinen ryhmä **Domain Users**:



Uuden paikallisen ryhmän luominen tehdään valitsemalla ensin **Käyttäjien hallinta** (User Manager)-ikkunasta uuden ryhmän jäseniksi haluamasi käyttäjätunnukset. Valitse **Käyttäjä | Uusi paikallinen ryhmä** (User | New Local Group). Jos valitsit yhden tai useamman käyttäjätunnuksen, valitut käyttäjät tulevat uuden ryhmän jäseniksi. Saat lueteltujen käyttäjätunnusten koko nimet näyttöön valitsemalla **Näytä koko nimet** (Show Full Names).

Kirjoita **Ryhmän nimi** (Group Name) -ruutuun uuden ryhmän nimi; millään muulla hallittavan toimialueen tai työaseman käyttäjällä tai ryhmällä ei saa olla samaa nimeä, eikä nimessä saa olla merkkejä " / \ [ ] : ; | = , + * ? < > .



Kirjoita **Kuvaus** (Description)-ruutuun uuden ryhmän kuvaus. Lisää jäseniä paikalliseen ryhmään valitsemalla **Lisää** (Add)-painike.

Voit myös valita **Käyttäjä | Uusi paikallinen ryhmä** (User | New Local Group) ja lisätä käyttäjät tässä vaiheessa yksitellen. Voit lisätä ryhmään käyttäjätunnuksia ja yleisiä ryhmiä sekä käytössä olevasta toimialueesta että luotetuista toimialueista.

Jos haluat poistaa jäseniä paikallisesta ryhmästä kaksoisnapauta ryhmän päälle tai valitse **Käyttäjä | Ominaisuudet** (User | Properties). Valitse yksi tai useampi nimi **Jäsenet** (Members)-ruudusta ja valitse **Poista** (Remove)-painike. Valitse lopuksi **OK**.

Yleisten ryhmien hallinta

User Manager for Domains hallitsee paitsi paikalliset, myös **yleiset ryhmät** (Global Groups) ja **-käyttäjät**. Yleinen ryhmä ja yleinen käyttäjä näkyvät luottosuhteen yli toisessakin toimialueessa ja paikallisen toimialueen NT-työasemassa; **toimialueen paikallinen käyttäjä** tai **paikallinen ryhmä** eivät näy eikä niitä voida lisätä toisen toimialueen tai paikallisen toimialueen NT-työaseman käyttäjäryhmiin.

Voit vaihtaa toimialuetta valitsemalla **User** | **Select Domain**.

Voit hallita myös NT-työasemaa kirjoittamalla hallittavan toimialueen nimeksi **työaseman nimi**, esimerkiksi **WS2**.

Toimialueen yleisiä ryhmiä ovat mm. **Domain Users** peruskäyttäjille ja **Domain Admins** pääkäyttäjille hallintakäyttöä varten.

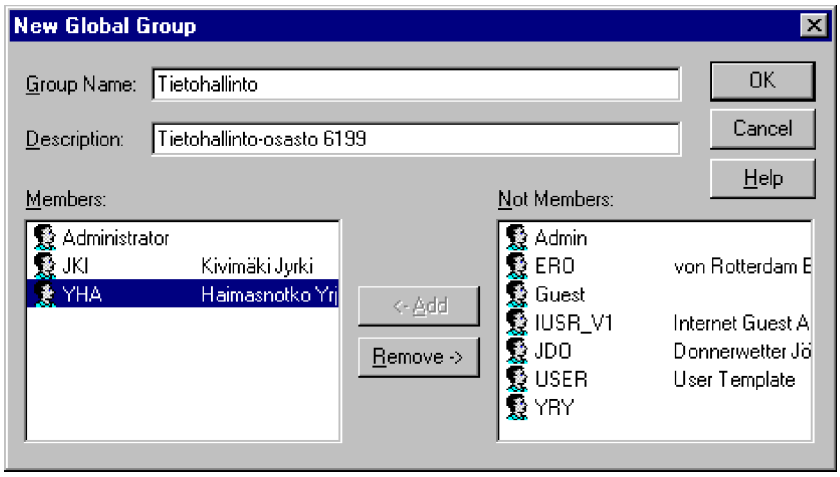
Uuden yleisen ryhmän luominen tehdään valitsemalla **User** | **New Global Group**.

Tähän ryhmään voit lisätä käyttäjät sitten yksitellen.

Jos valitsit ennen ryhmän luomista yhden tai useamman käyttäjätunnuksen, valitut käyttäjät tulevat uuden ryhmän jäseniksi.

Kirjoita **Group Name** -ruutuun uuden ryhmän nimi; millään muulla hallittavan toimialueen tai työaseman käyttäjällä tai ryhmällä ei saa olla samaa nimeä eikä nimessä saa olla merkkejä " / \ [ ] : ; | = , + * ? < > .

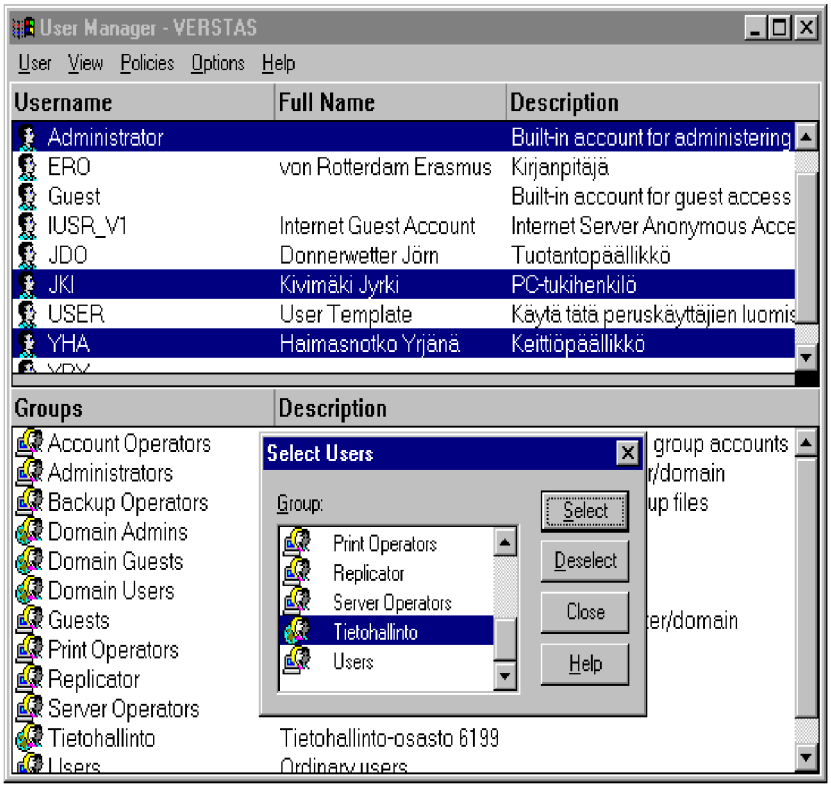
Kirjoita **Description**-ruutuun uuden ryhmän kuvaus. Lisää jäseniä paikalliseen ryhmään valitsemalla **Add**-painike. Voit lisätä yleiseen ryhmään yleisiä ja paikallisia käyttäjätunnuksia käytössä olevasta toimialueesta.



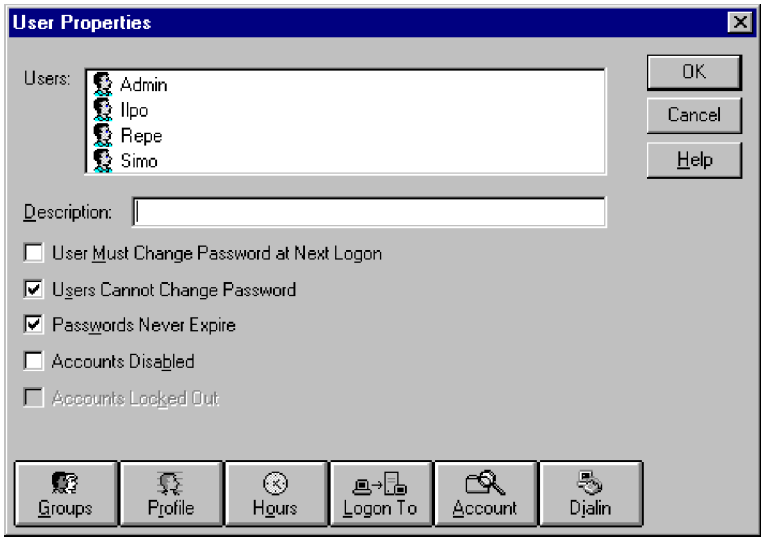
Jos haluat poistaa jäseniä ryhmästä, kaksoisnapauta ryhmän päälle tai valitse **User | Properties**. Valitse yksi tai useampi nimi **Members**-ruudusta ja valitse **Remove**-painike. Valitse lopuksi **OK**.

Ryhmään kuuluvien käyttäjien etsiminen

Voit etsiä ryhmään kuuluvat käyttäjät valitsemalla **User** | **Select Users**.



Voit valita useamman ryhmän. Tällöin valinta kohdistuu niihin käyttäjätunnuksiin, jotka ovat jonkin valitun ryhmän jäseniä.



Tämän jälkeen voit painaa **Enter** tai valita **User** | **Properties**, niin pääset muuttamaan kaikkien valittujen käyttäjien yhteisiä asetuksia.

Käytännöt ja niiden hallinta

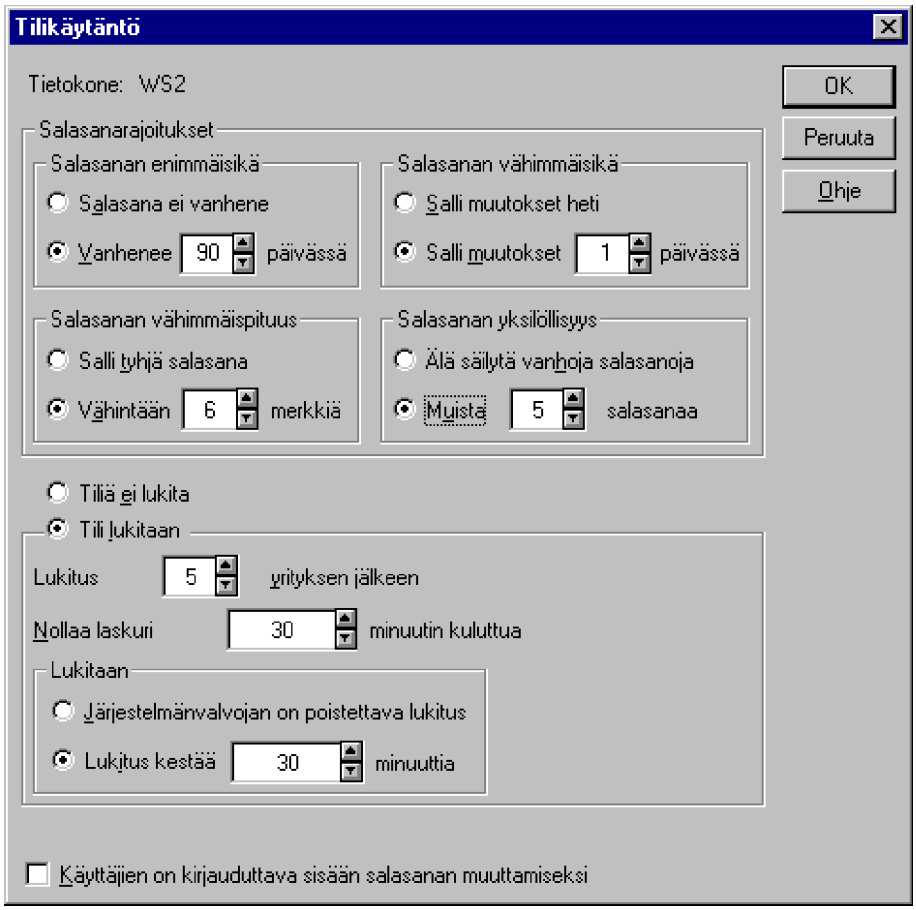
On asetettavissa erilaisia yleisiä, kaikkia käyttäjiä koskevia asetuksia; näitä ovat tilikäytäntö **Account Policy**, käyttöoikeuskäytäntö **User Rights** ja valvontakäytäntö **Audit Policy**.

Windows NT -työasemassa asetukset vaikuttavat vain kyseiseen NT-työasemaan; NT-toimialueella asetukset ovat toimialueen laajuisia, eli ne vaikuttavat kaikkiin toimialueen **ohjauskoneisiin** (*Domain Controller*).

Koska voit käsitellä myös suomenkielisessä Windows NT 4.0-työasemassa näitä käytäntöjä, esittelen myös suomenkieliset komennot.

Tilikäytäntö

Suojauskäytännöt asetetaan valinnalla **Käytännöt | Tili** (Policies | Account). Käytäntö valvoo kaikkien käyttäjätunnusten salasanojen käyttöä ja ne eroavat vain hieman NT 4.0 työaseman ja palvelimen välillä.



Asetukset ovat seuraavat:

- **Salasanan enimmäisikä** (Maximum Password Age) - anna arvo **1 - 999** tai valitse **Salasana ei vanhene** (Password Never Expires)

- **Salasanan vähimmäisikä** (Minimum Password Age) - Anna arvo **1 - 999** tai valitse **Salli muutokset välittömästi** (Allow Changes Immediately). Jos valitset vaihtoehdon **Salli muutokset välittömästi**, valitse **Salasanan yksilöllisyys** (Password Uniqueness) -asetuksista **Älä säilytä vanhoja salasanoja** (Do Not Keep Password History)

- **Salasanan vähimmäispituus** (Minimum Password Length) - anna arvo **1 - 14** tai valitse **Salli tyhjä salasana** (Permit Blank Password), jolloin salasana voi olla tyhjä eli sitä ei ole

- **Salasanan yksilöllisyys** (Password Uniqueness) - anna arvo **1 - 8** tai valitse **Älä säilytä vanhoja salasanoja** (Do Not Keep Password History). Jos määrität esimerkiksi arvon **Muista 4 salasanaa** (Remember 4 Passwords), määritä **Salasanan vähimmäisikä** (Minimum Password Age)-ryhmään muutosten sallimisaika esimerkiksi **Salli muutokset 14 päivässä** (Allow Changes In 14 Days)

Kun käyttäjän salasana vanhenee, siitä tulee käyttäjälle ilmoituksia oletuksena 14 vuorokautta aiemmin. Seuraavan asetuksen voi lisätä ja muuttaa rekisteristä:

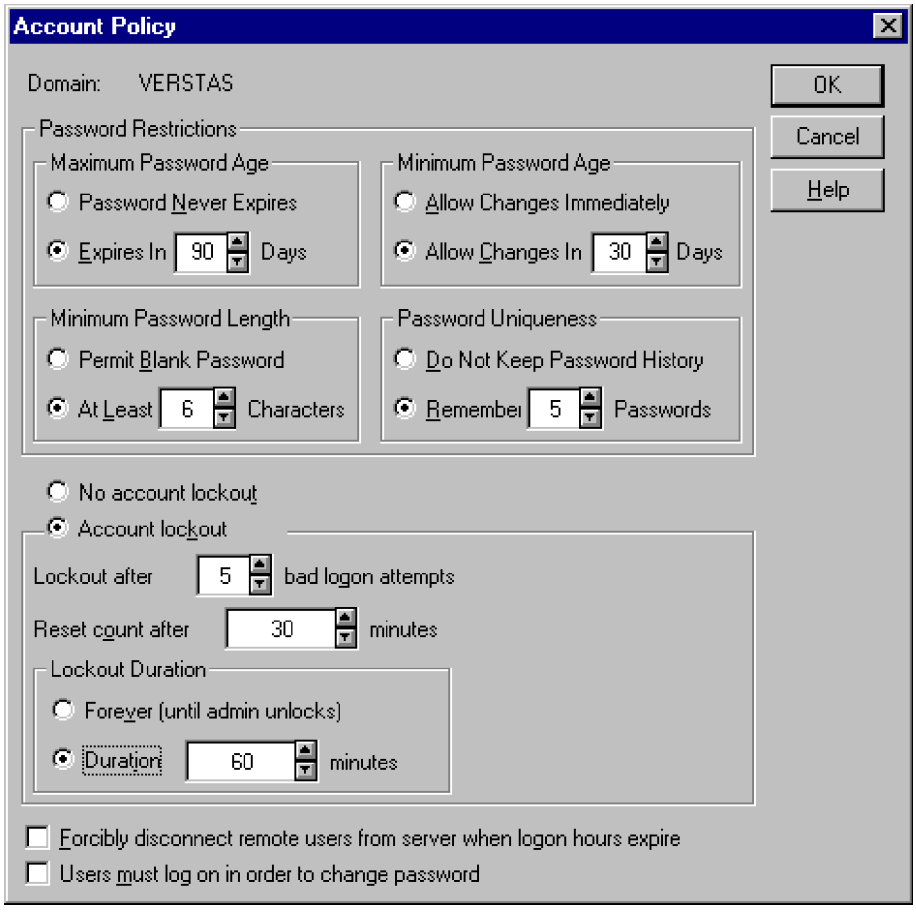
Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**PasswordExpiryWarning**
Tyyppi	**REG_DWORD**
Arvo	**Päivien lukumäärä (oletus 14)**

Jos valitset **Tili lukitaan** (Account lockout), voit antaa asetuksia käyttäjätunnusten lukitsemiseen:

- **Lukitus ... yrityksen jälkeen** (Lockout after bad logon attempts) yrityskerrat, joiden jälkeen käyttäjätunnus lukitaan, eikä sillä voi yrittää kirjautua käyttäjäksi, ennen kuin lukitus on poistettu kyseisestä käyttäjätunnuksesta **Käyttäjien hallinnalla** (User Manager). Arvo voi olla **1-999**

- **Nollaa laskuri ... minuutin kuluttua** (Reset count after minutes) - edellinen laskuri nollataan annettujen minuuttien jälkeen; arvo voi olla **1-99999**

- **Lukitaan** (Lockout Duration) lukituksen kesto: **Järjestelmänvalvojan on poistettava lukitus** (Forever (until admin unlocks) kunnes pääkäyttäjä poistaa lukituksen tai **Lukitus kestää ... minuuttia** (Duration minutes) tietty aika minuutteina; arvo on **1-99999**.



- **Käyttäjien on kirjauduttava sisään salasanan muuttamiseksi** (Users must log on in order to change password) - käyttäjän on kirjauduttava ennen kuin voi muuttaa salasanaansa.

Lisäksi NT-palvelimessa on asetus:

- **Forcibly disconnect remote users from server when logon hours expire** - jos asetus on valittu, tällöin käyttäjän **Aika** (Hours)-asetuksissa annetaan paitsi sallittu kirjautumisaika, myös sallittu toimialueella kirjautumisaika.

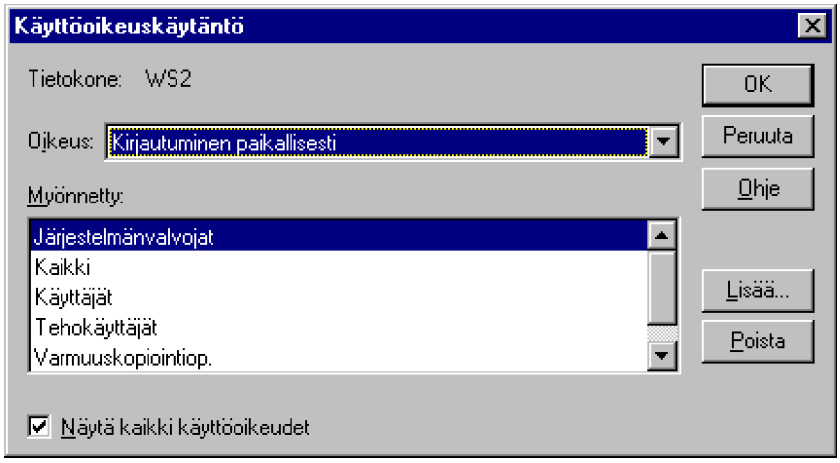
Käyttöoikeuskäytäntö

Käyttöoikeuskäytäntö (User Rights Policy) valvoo ryhmille ja käyttäjätunnuksille myönnettyjä oikeuksia. Myönnettyjen oikeuksien avulla käyttäjä voi tehdä erilaisia toimintoja työasemassaan ja toimialueella.

Yleensä helpointa on myöntää oikeuksia lisäämällä käyttäjätunnus sellaiseen ryhmään, jolla on jo tarvittavat oikeudet. Tämä on huomattavasti kätevämpää kuin oikeuksien myöntäminen käyttöoikeuskäytännön avulla. Jos muutat kovin paljon oletusasetuksia, saatat saada järjestelmäsi hallitsemattomaan tilaan. Koska suojaukset ovat NT-konekohtaisia, käsittelen myös suomenkielisen Windows NT 4.0-työaseman.

Katso myös suojauksia käsittelevä **Luku 11**.

Valitse **Käytännöt | Käyttäjien oikeudet** (Policies | User Rights Policy). Valitse haluamasi käyttöoikeus **Oikeus** (Right)-ruudusta.



Käyttäjien oikeuksia ovat seuraavat (järjestys on suomenkielisen Windows NT 4.0:n mukainen valinnalla **Näytä kaikki käyttöoikeudet** (Show Advanced User Rights)):

- **Aikaprioriteetin kasvatus** (Increase scheduling priority) - käyttäjällä on oikeus muuttaa prosessin suorituksen prioriteettia. Oikeudet oletuksena: **Järjestelmänvalvojat** (Administrators), **Tehokäyttäjät** (Power Users).

- **Järjestelmän ajan muuttaminen** (Change the system time) - käyttäjällä on oikeus muuttaa järjestelmän kellonaikaa. Oikeudet oletuksena: **Järjestelmänvalvojat** (Administrators), **Tehokäyttäjät** (Power Users). Huomaa! Jos kirjauskomentojonossa on komento **NET TIME /SET**, käyttäjällä on oltava tämä oikeus NT-työasemassa; muuten komento aiheuttaa virheilmoituksen.

- **Järjestelmän sammutus** (Shut down the system) - käyttäjällä on oikeus sammuttaa NT. Oikeudet oletuksena NT-palvelimessa: **Järjestelmänvalvojat** (Administrators), **Varmuuskopiointiop.** (Backup Operators), **Tilioperaattorit** (Account Operators), **Tulostusoperaattorit** (Print Operators), **Palvelinoperaattorit** (Server Operators).

- Oikeudet oletuksena NT-työasemassa: **Järjestelmänvalvojat** (Administrators), **Varmuuskopiointiop.** (Backup Operators), **Kaikki** (Everyone), **Tehokäyttäjät** (Power Users), **Käyttäjät** (Users). Huomaa, että palvelinta ei voi **Käyttäjä** (User) sammuttaa - toisaalta **Käyttäjällä** ei ole myöskään oikeuksia kirjautua palvelimeen paikallisesti käyttäjäksi.

- **Kiintiöiden kasvatus** (Increase quotas) - oikeudella ei ole merkitystä nykyisillä NT-versioilla.

- **Järjestelmän suoritustason määritys** (Profile system performance) - oikeus ajaa järjestelmän suorituskyvyn seurantaa. Oikeudet oletuksena NT-palvelimessa ja NT-työasemassa: **Järjestelmänvalvojat** (Administrators).

- **Kirjautuminen komentojonotyönä** (Log on as a batch job) - oikeudella ei ole merkitystä nykyisillä NT-versioilla.

- **Kirjautuminen paikallisesti** (Log on locally) - käyttäjä voi kirjautua käyttäjäksi a.o. NT-tietokoneen näppäimistöltä. Oikeudet oletuksena NT-palvelimessa: **Järjestelmänvalvojat** (Administrators), **Varmuuskopiointiop.** (Backup Operators), **Tilioperaattorit** (Account Operators), **Tulostusoperaattorit** (Print Operators), **Palvelinoperaattorit** (Server Operators). Oikeudet oletuksena NT-työasemassa: **Järjestelmänvalvojat** (Administrators), **Varmuuskopiointiop.** (Backup Operators), **Kaikki** (Everyone), **Tehokäyttäjät** (Power Users), **Käyttäjät** (Users), **Vieraat** (Guests).

- **Kirjautuminen palveluna** (Log on as a service) - prosessi voi rekisteröityä järjestelmään palveluna näillä käyttäjätunnuksilla. Oletuskäyttäjiä ei ole. Jotkut sovellukset edellyttävät tällaista oikeutta määritellyille käyttäjätunnuksille, esimerkiksi **MS Exchange** tai **MS SQL Server**. Kannattaa siis lukea sovelluksen käsikirjat!

- **Käyttöjärjestelmän osanan toimiminen** (Act as part of the operating system) joillakin alijärjestelmillä on tämä oikeus, muita oletuskäyttäjiä ei ole.

- **Laiteohjaimien lataus muistiin ja muistista poisto** (Load and unload device drivers) - käyttäjällä on oikeus ladata ja poistaa laiteohjaimia. Oletuskäyttäjä: **Järjestelmänvalvojat** (Administrators)

- **Laitteiston ympäristöarvojen muuttaminen** (Modify firmware environment variables) - CMOS-RAM:issa sijaitsevien järjestelmäasetusten muuttaminen. Oletuskäyttäjä: **Järjestelmänvalvojat** (Administrators)

- **Muistissa olevien sivujen lukinta** (Lock pages in memory) - käyttäjä voi lukita keskusmuistissa olevat sivut siten, että niitä ei sivuteta sivutustiedostoon (**Pagefile.sys**). Oletuskäyttäjiä ei ole.

- **Ohjelmien virheentarkistus** (Debug programs) - käyttäjällä on oikeus debugata esimerkiksi säikeitä (threads). Oletuskäyttäjä: **Järjestelmänvalvojat** (Administrators).

- **Poikittaistarkistuksen ohitus** (Bypass traverse checking) - käyttäjällä on pääsy alihakemistoihin ja tiedostoihin, vaikka ei olisikaan käyttöoikeutta päähakemistotasolla. Oletuskäyttäjä: **Kaikki** (Everyone).

- **Prosessitason tunnussanoman korvaus** (Replace a process-level token) - käyttäjällä on oikeus muuttaa prosessitason suojausmäärityksiä (*security-access token*). Vain järjestelmätasolla on tämä oikeus. Oletuskäyttäjiä ei ole.

- **Pysyvien jaettujen objektien luonti** (Create permanent shared objects) - käyttäjällä on oikeus luoda NT:n sisäisiä erityisiä jaettuja objekteja (johin pääsee käsiksi esimerkiksi tunnuksella \\laite). Oletuskäyttäjiä ei ole.

- **Sammutuksen pakotus etäjärjestelmästä** (Force shutdown from a remote system) - käyttäjällä on oikeus sammuttaa järjestelmä toisesta tietokoneesta. Oikeudet oletuksena NT-palvelimessa: **Järjestelmänvalvojat** (Administrators) ja **Palvelinoperaattorit** (Server Operators). Oikeudet oletuksena NT-työasemassa: **Järjestelmänvalvojat** (Administrators) ja **Tehokäyttäjät** (Power Users).

- **Sivutustiedoston luonti** (Create a pagefile) - oikeudella ei ole merkitystä nykyisillä NT-versioilla.

- **Suojausvalvontojen tekeminen** (Generate security audits) - oikeus luoda lokivientejä suojauslokiin (*security-audit log*). Oletuskäyttäjiä ei ole.

- **Tiedostojen ja hakemistojen palautus** (Restore files and directories) - oikeus palauttaa varmistettuja tiedostoja ja hakemistoja ohittaen tiedosto- ja hakemistotason oikeudet. Oikeudet oletuksena NT-palvelimessa: **Järjestelmänvalvojat** (Administrators), **Varmuuskopiointiop.** (Backup Operators) ja **Palvelinoperaattorit** (Server Operators). Oikeudet oletuksena NT-työasemassa: **Järjestelmänvalvojat** (Administrators) ja **Varmuuskopiointiop.** (Backup Operators).

- **Tiedostojen ja hakemistojen varmuuskopiointi** (Back up files and directories) - oikeus varmistaa varmistettuja tiedostoja ja hakemistoja ohittaen tiedosto- ja hakemistotason oikeudet.

Oikeudet oletuksena NT-palvelimessa: **Järjestelmänvalvojat** (Administrators), **Varmuuskopiointiop.** (Backup Operators) ja **Palvelinoperaattorit** (Server Operators). Oikeudet oletuksena NT-työasemassa: **Järjestelmänvalvojat** (Administrators) ja **Varmuuskopiointiop.** (Backup Operators).

- **Tiedostojen tai muiden objektien omistukseen otto** (Take ownership of files or other objects) - oikeus ottaa objekteja omistukseen ohittaen objektien suojausasetukset. Oletuskäyttäjä: **Järjestelmänvalvojat** (Administrators).

- **Tietokoneen käyttö verkosta** (Access this computer from the network) - käyttäjä voi kytkeytyä tietokoneeseen verkon kautta. Oikeudet oletuksena NT-palvelimessa: **Järjestelmänvalvojat** (Administrators) ja **Kaikki** (Everyone). Oikeudet oletuksena NT-työasemassa: **Järjestelmänvalvojat** (Administrators) ja **Kaikki** (Everyone).

- **Tunnussanomaobjektin luonti** (Create a token object) - oikeudet luoda suojausjärjestelmän tunnussanomia (*access token*). Vain järjestelmän LSA (Local Security Authority) voi luoda näitä. Oletuskäyttäjiä ei ole.

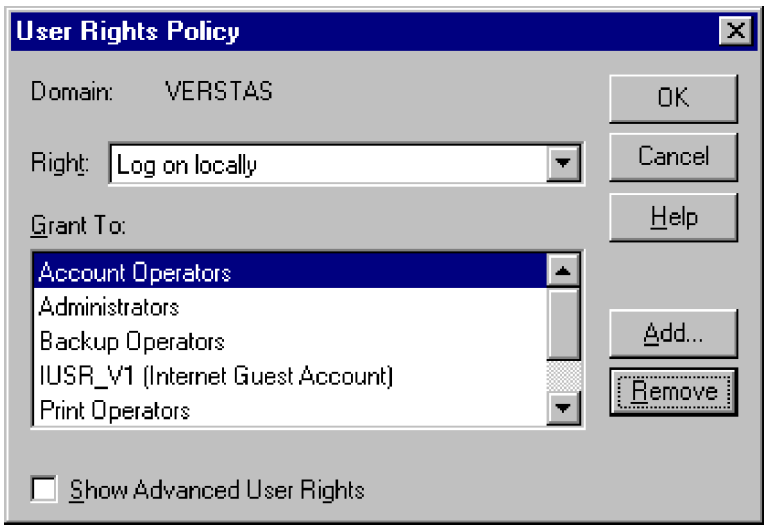
- **Työaseman lisääminen toimialueelle** (Add workstations to the domain) - ei kuitenkaan merkitystä Windows NT:ssä. Oletuskäyttäjiäkään ei ole. Työaseman lisääminen tehdään **Palvelimen hallinnalla** (Server Manager).

- **Valvonta- ja suojauslokin hallinta** (Manage auditing and security log) - oikeus hallita suojauslokia, mutta ei kuitenkaan asettaa lokia käyttöön **Käyttäjien hallinnassa** (User Manager). Oletuskäyttäjä: **Järjestelmänvalvojat** (Administrators).

- **Yksittäisen prosessin määritys** (Profile single process) - oikeus ajaa prosessin suorituskyvyn seurantaa. Oikeudet oletuksena NT-palvelimessa: **Järjestelmänvalvojat** (Administrators). Oikeudet oletuksena NT-työasemassa: **Järjestelmänvalvojat** (Administrators) ja **Tehokäyttäjät** (Power Users).

On kaksi asetusta, joita ainakin saattaa joutua muuttamaan:

- **Kirjautuminen paikallisesti** (Log on locally) - tähän saattaa joutua lisäämään käyttäjiä, joille halutaan antaa oikeudet kirjautua esimerkiksi palvelimeen käyttäjänä palvelimen näppäimistöltä.



- **Kirjautuminen palveluna** (Log on as service) - tähän saattaa joutua lisäämään **MS Systems Managment Serverin** tai **MS Exchangen** käyttäjätunnuksen.

Huomattavaa:

- Kun valitset oikeuden, **Myönnetty** (Grant)-ruutuun tulee luettelo ryhmistä ja käyttäjätunnuksista, joille kyseinen oikeus on myönnetty.

- Voit lisätä saman oikeuden muille ryhmille tai käyttäjätileille valitsemalla **Lisää** (Add)-painikkeen ja kirjoittamalla tarvittavat tiedot **Lisää käyttäjiä ja ryhmiä** (Add Users and Groups)-valintaikkunaan.

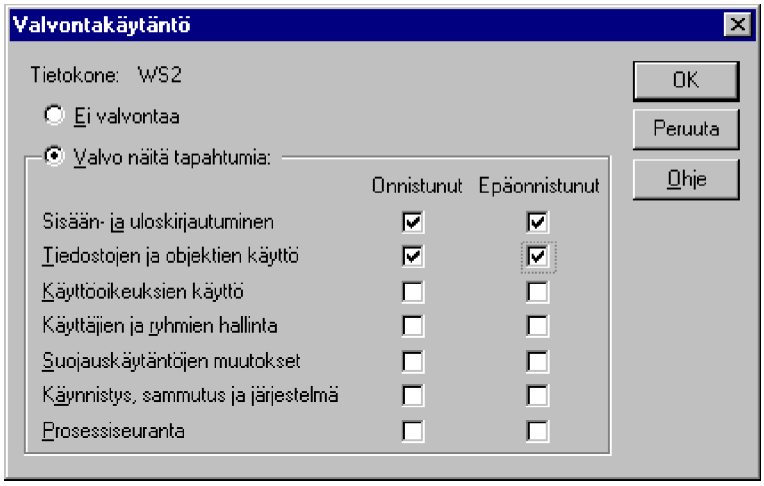
- Jos haluat poistaa oikeuden ryhmältä tai käyttäjätililtä, valitse ensin **Myönnetty** (Grant)-ruudusta haluamasi nimi ja sitten **Poista** (Remove)-painike.

- Jos haluat tarkastella **kaikkia käyttöoikeuksia**, valitse **Näytä kaikki käyttöoikeudet** (Show Advanced User Rights). Täältä löytyy esimerkiksi **Kirjautuminen palveluna** (Log on as service).

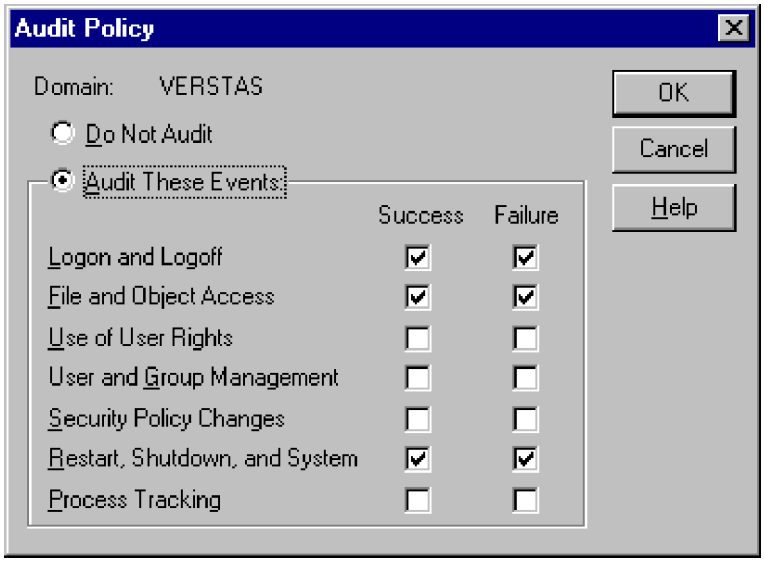
Valvontakäytäntö

NT:ssä seurataan käyttäjien tekemiä toimia valvomalla **suojaustapahtumia** ja lisäämällä **tapahtumamerkinnät suojauslokiin** (Security Log). Näitä tapahtumia ovat esimerkiksi käyttäjien sisään- ja uloskirjautumiset ja tiedostojen käyttöyritykset. Lokiin voidaan tallentaa sekä **onnistuneet** että **epäonnistuneet** yritykset.

Valvontakäytännön (Audit Policy) avulla määritetään lokiin merkittävät suojaustapahtumat.



Toimialueita valvottaessa valvontakäytäntö vaikuttaa toimialueen ohjauskoneiden suojauslokeihin, **koska ne käyttävät samaa valvontakäytäntöä;** NT-työasemaa valvottaessa valvontakäytäntö vaikuttaa vain kyseisen työaseman suojauslokiin.



Valvontakäytännön hallinta tehdään valitsemalla **Käytännöt | Valvonta** (Policies | Audit).

Koska suojauslokin koko on rajattu, valitse tarkkaan kirjattavat tapahtumat; suojauslokin enimmäiskoko on määritetty **Tapahtumien valvonnassa** (Event Viewer), jossa myös suojauslokin merkintöjä voi tarkastella.

Jos haluat tallentaa tapahtumia suojauslokiin, valitse **Valvo näitä tapahtumia** (Audit These Events). Jos et halua tallentaa tapahtumia, valitse **Ei valvontaa** (Do Not Audit). Määritä tallennettavat tapahtumat valitsemalla haluamillesi tapahtumille **Onnistunut** (Success) tai **Epäonnistunut** (Failure) tai poista niiden valinta.

Valittavat tapahtumat ovat seuraavat:

- **Sisään- ja uloskirjautuminen** (Logon and Logoff) - onnistuneet tai epäonnistuneet kirjausyritykset. Suojauslokin jokaisessa tapahtumassa on lisäksi selvitetty onko kyseessä **vuorovaikutteinen** (interactive), **verkon kautta suoritettu** (network) vai **palvelun** (service) kirjausyritys.

- **Tiedostojen ja objektien käyttö** (File and Object Access) - onnistuneet ja epäonnistuneet suojattujen objektien käyttöyritykset.

- **Käyttöoikeuksien käyttö** (Use of User Rights) - onnistuneet ja epäonnistuneet käyttöoikeuksien saantiyritykset sekä milloin ne on annettu. Pätee vain saantiaikaan, ei käyttöaikaan.

- **Käyttäjien ja ryhmien hallinta** (User and Group Management) - käyttäjätietokannan muutokset, kuten käyttäjän luominen ja ryhmäjäsenyyksien muuttaminen.

- **Suojauskäytäntöjen muutokset** (Security Policy Changes) - muutokset suojauskäytäntötietokantaan, kuten kirjauskäytäntöjen muuttaminen.

- **Käynnistys, sammutus ja järjestelmä** (Restart, Shutdown, and System) - koko järjestelmän suojauksiin vaikuttavat toiminnot, kuten järjestelmän sammutus/käynnistys.

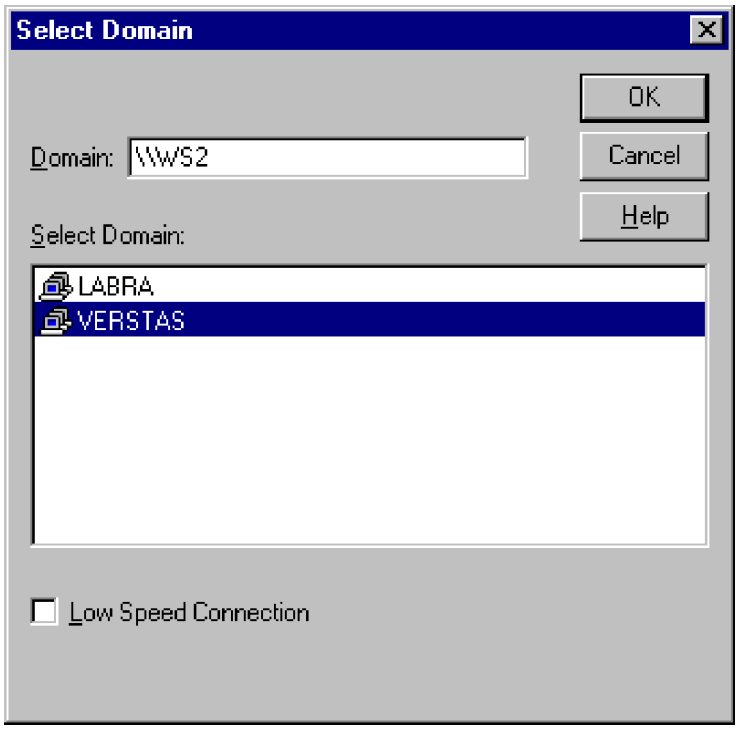
- **Prosessiseuranta** (Process Tracking) - yksityiskohtaiset

tiedot prosesseista.

Älä aseta tarpeettomia tapahtumia valvottavaksi: saatat hidastaa järjestelmän toimintaa jopa 20% valitsemalla kaikki tapahtumat!

Toimialueen valitseminen

User Manager for Domainsissa voit vaihtaa toimialuetta valitsemalla **User** | **Select Domain**. Voit hallita myös NT-työaseman käyttäjätietokantaa kirjoittamalla hallittavan toimialueen nimeksi **työaseman nimi**, esimerkiksi **WS2**.



Voit vaihtaa toimialuetta seuraavasti:

1) Valitse **Computer** | **Select Domain**

2) Valitse toimialue **Select Domain**-luettelosta tai kirjoita sen nimi **Domain**-ruutuun; voit antaa **yksittäisen NT-työaseman/palvelimen** nimen kirjoittamalla **nimi**

3) Jos olet yhteydessä toimialueeseen, työryhmään tai työasemaan/palvelimeen **hitaan tiedonsiirtoyhteyden kautta** (esi-

merkiksi **RAS**), valitse vaihtoehto **Low Speed Connection**. Kun annat nimen, asetuksen mahdollinen aiempi arvo tulee näkyviin. Jos aiempi asetus ei ole tiedossa, vaihtoehto ei aluksi ole valittuna. Voit hyväksyä asetuksen tai muuttaa sitä

4) Valitse lopuksi **OK**.

Luottosuhteet

Luottosuhteen muodostaminen tapahtuu kahdessa vaiheessa. Ensin yhden toimialueen on annettava toisen toimialueen luottaa siihen. Sitten toinen toimialue on määritettävä luottamaan ensimmäiseen toimialueeseen. Koska luottosuhdetta ei ole vielä muodostettu, kahden eri järjestelmänvalvojan on ehkä erikseen tehtävä nämä vaiheet.

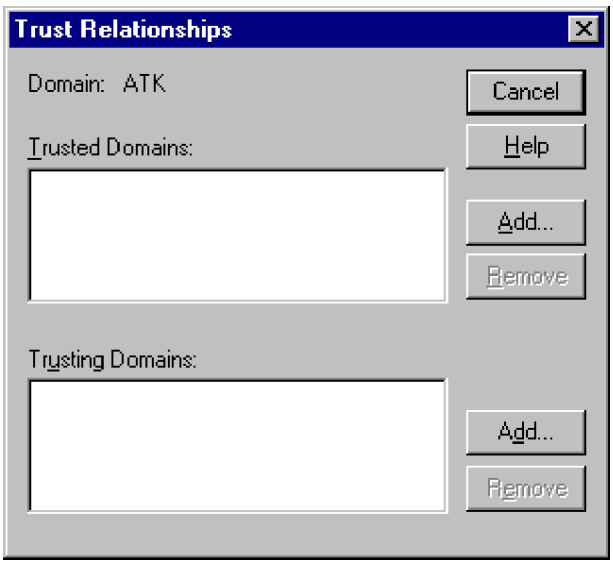
Esimerkissä on kaksi toimialuetta: **VERSTAS** ja **ATK**. Halutaan järjestää luottosuhteet siten, että **VERSTAS** luottaa **ATK**:hon. Tällöin ATK-toimialueen yleisille käyttäjätunnuksille ja yleisille käyttäjäryhmille voidaan antaa oikeuksia VERSTAS-toimialueella.

Lisäksi ATK-toimialueen yleisille käyttäjätunnuksille ja yleisille käyttäjäryhmille voidaan määritellä ryhmäjäsenyyksiä VERSTAS-toimialueen paikallisiin ryhmiin.

Luottamisen salliminen toimialueeseen

Luottamisen salliminen toimialueeseen tehdään seuraavasti:

1) Valitse **ATK**-toimialueessa **Policies | Trust Relationships**. **Trust Relationships**-valintaikkunassa on toimialueen luottosuhdeluettelo. Jos luottosuhteita ei ole, luettelo on tyhjä

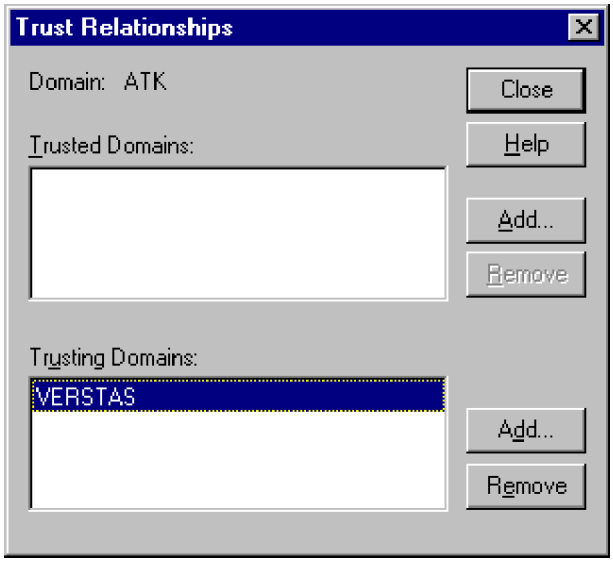


2) Valitse **Trusting Domains** -ruudun vieressä oleva **Add**-painike.

Kirjoita **Domain to Permit** -ruutuun sen toimialueen nimi, joka saa luottaa tähän toimialueeseen. Nimen voi kirjoittaa joko isoin tai pienin kirjaimin; näytössä se kuitenkin näkyy aina isoin kirjaimin kirjoitettuna.

Kirjoita luottosuhteen perustamisessa tarvittava salasana sekä **Password**- että **Confirm Password**-ruutuun. Salasana ei ole pakollinen. Jos käytät salasanaa, niin muista, että salasanojen kirjainkoko on merkitsevä, koska NT erottaa isot ja pienet kirjaimet salasanoissa!

3) Valitse **Domain to Permit** -valintaikkunasta **OK**. Lisätty nimi näkyy **Trust Relationships** -valintaikkunan **Permitted to Trust this Domain**-ruudussa



4) Valitse **Trust Relationships**-valintaikkunasta **Close**-painike.

5) Ilmoita edellä annettu salasana sen toimialueen pääkäyttäjälle, jonka sallitaan luottaa tähän toimialueeseen. Toisen toimialueen järjestelmänvalvojan on tehtävä luottosuhdemäärityksen seuraava vaihe, jossa toimialue määritetään luottamaan tähän toimialueeseen.

Nyt on mahdollistettu **ATK**-toimialueessa sellaisen luottosuhteen muodostuminen, jossa **VERSTAS**-toimialue voi luottaa **ATK**-toimialueeseen.

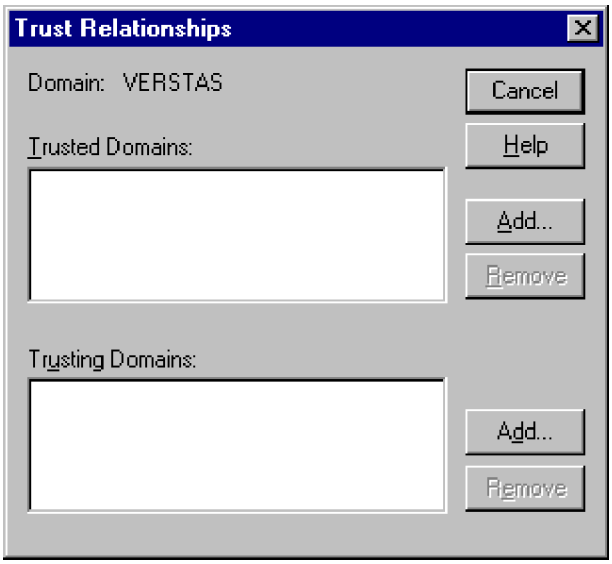
Luotettujen toimialueiden määrittäminen

Luottosuhteen muodostaminen tapahtuu kahdessa vaiheessa: ensin yhden toimialueen on annettava toisen toimialueen luottaa siihen ja määriteltävä salasana, jolla luottosuhde voidaan muodostaa. Sitten toinen toimialue on määritettävä luottamaan ensimmäiseen toimialueeseen. Koska luottosuhdetta ei ole vielä muodostettu, mahdollisesti kahden eri pääkäyttäjän on tehtävä nämä vaiheet.

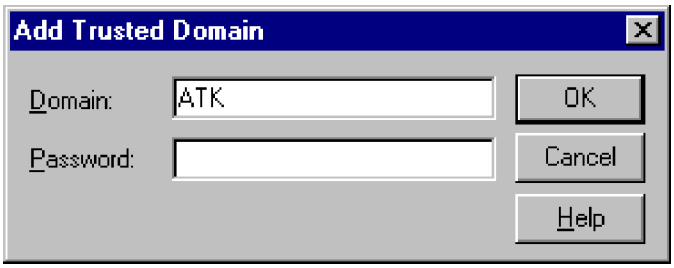
Jatkaakseni edellistä esimerkkiä, seuraavaksi **VERSTAS**-toimialueessa määritellään **ATK** luotetuksi toimialueeksi:

1) Pyydä salasana luotetun toimialueen pääkäyttäjältä (**ATK**-toimialueen pääkäyttäjä)

2) Valitse **VERSTAS**-toimialueessa **Policies** | **Trust Relationships**. **Trust Relationships** -valintaikkunassa on toimialueen luottosuhdeluettelo

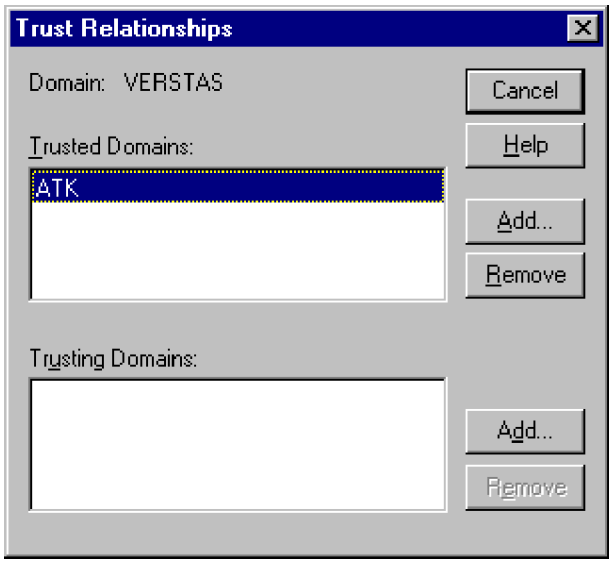


3) Valitse **Trusted Domains** -ruudun vieressä oleva **Add**-painike. Kirjoita **Domain** -ruutuun sen toimialueen nimi, johon luotetaan. Nimen voi kirjoittaa joko isoin tai pienin kirjaimin; näytössä se kuitenkin näkyy aina isoin kirjaimin kirjoitettuna. Kirjoita luottosuhteen perustamisessa tarvittava salasana **Password**-ruutuun. Salasanojen kirjainkoko on merkitsevä, koska NT erottaa isot ja pienet kirjaimet salasanoissa! Paina **OK**



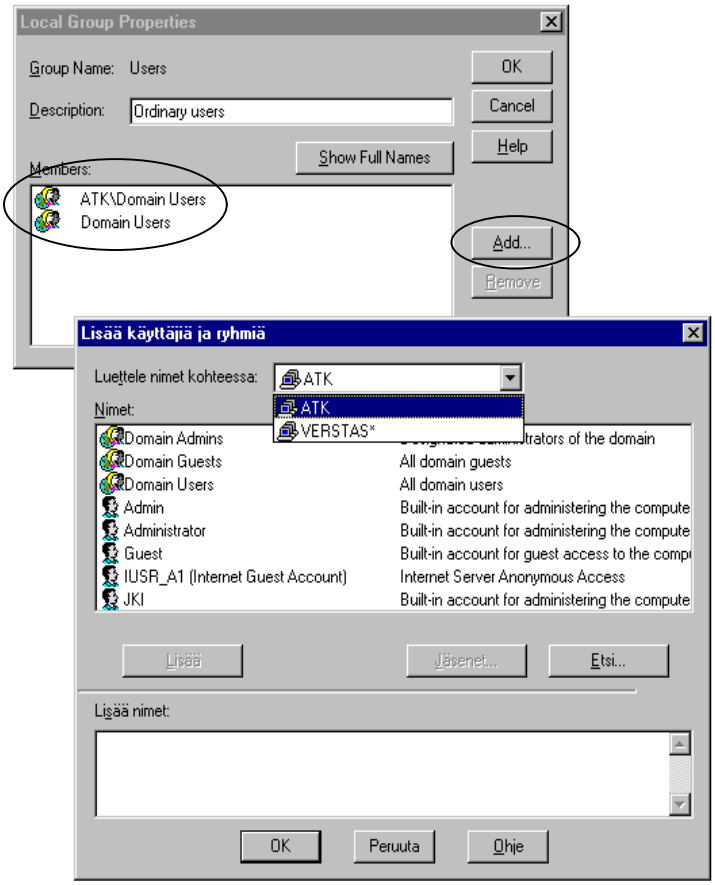
4) Saat ilmoituksen luottosuhteen onnistumisesta, jos kaikki meni hyvin

5) Lisätty nimi näkyy **Trusted Domains** -ruudussa.

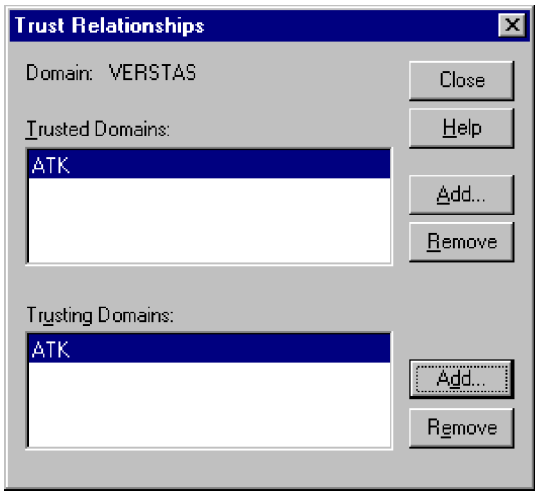


6) Valitse **Trust Relationships**-valintaikkunassa **Close**-painike.

Tämän jälkeen voidaan **VERSTAS**-toimialueella vaikkapa lisätä **ATK**-toimialueen **Domain Users**-ryhmä **VERSTAS**-toimialueen **Users** -ryhmään, niin **ATK**-toimialueen käyttäjät pääsevät käyttämään kaikkia **VERSTAS**-toimialueella paikalliselle **Users**-ryhmälle jaettuja resursseja.



Voit myös sallia kaksisuuntaisen luottosuhteen siten, että myös **ATK** luottaa **VERSTAS**-toimialueeseen. Tämä on ns. täydellinen luottosuhde (*Complete Trust*)



Voit poistaa luottosuhteet valitsemalla halutun luottosuhteen kohdalla **Remove**.

Käyttäjätunnusten hallinta NET-komentojen avulla

Voit käyttää komentorivin **NET-komentoja** käyttäjätunnusten hallinnassa.

NET ACCOUNTS

Päivittää käyttäjätietokannan (*Account Database*) ja muuttaa tarvittaessa kaikkien käyttäjätunnusten salasana- ja kirjautumisvaatimuksia. Verkkokirjauspalvelun (**NET LOGON**) on oltava käynnissä koneella, jonka käyttäjätunnusten parametreja haluat muuttaa. Komennolla **NET ACCOUNTS** saat näyttöön nykyiset salasana-asetukset ja kirjautumisrajoitukset sekä tietoja toimialueesta.

Syntaksi:

NET ACCOUNTS [/FORCELOGOFF:{MINUUTTIA | EI}] [/MINPWLEN:PITUUS] [/MAXPWAGE:{PÄIVÄÄ | UNLIMITED}] [/MINPWAGE:PÄIVÄÄ] [/UNIQUEPW:MÄÄRÄ] [/DOMAIN]NET ACCOUNTS [/SYNC] [/DOMAIN]

Parametrit:

/FORCELOGOFF:{MINUUTTIA | EI}

Aika on se, mikä odotetaan käyttäjätunnuksen vanhennuttua tai sallitun kirjautumisajan päätyttyä, ennen kuin käyttäjän istunto palvelimella lopetetaan. Vaihtoehto ei poista pakollisen uloskirjauksen käytöstä; oletusarvo on **EI** (NO). Jos parametri **/FORCELOGOFF:MINUUTTIA** on määritetty, käyttäjää varoitetaan, ennen kuin hänet kirjataan ulos verkosta. Varoitus lähetetään arvon **minuuttia** verran ennen uloskirjausta; jos käyttäjällä on avoimia tiedostoja, häntä varoitetaan siitä. Jos määritetty aika on alle kaksi minuuttia, käyttäjää kehotetaan kirjautumaan ulos **heti.**

/MINPWLEN:PITUUS

Määrittää käyttäjätunnusten salasanojen vähimmäispituuden: sallitut arvot ovat **0 - 14** merkkiä; oletusarvo on **6** merkkiä

/MAXPWAGE:{PÄIVÄÄ | UNLIMITED}

Määrittää enimmäisajan, jonka käyttäjätunnuksen salasana voi olla voimassa. Jos arvo on **UNLIMITED**, rajoitus ei ole käytössä. Määritetyn **/MAXPWAGE**-arvon on oltava suurempi kuin määritetyn **/MINPWAGE**-arvon. Sallitut arvot ovat **1 - 49 710** päivää ja **UNLIMITED**; oletusarvo on **90** päivää

/MINPWAGE:PÄIVÄÄ

Vähimmäisaika, minkä uuden salasanan on oltava voimassa, ennen kuin sitä voidaan muuttaa. Jos arvo on **0**, rajoitus **ei ole käytössä**. Sallitut arvot ovat **0 - 49 710** päivää. Oletusarvo on **0** päivää

/UNIQUEPW:MÄÄRÄ

Estää käyttäjää käyttämästä samaa salasanaa uudelleen, ennen kuin salasana on muutettu **MÄÄRÄ** kertaa. Sallitut arvot ovat **0 - 8** salasanan muutoskertaa ja oletusarvo on **5** muutoskertaa

/DOMAIN

Suorittaa toiminnon toimialueen PDC:ssä; muussa tapauksessa toiminto suoritetaan paikallisessa työasemassa. Tätä parametria käytetään vain niissä NT-koneissa, jotka kuuluvat toimialueeseen ja joihin **ei ole** asennettu NT Server -ohjelmistoa; oletusarvona on, että NT Serverit suorittavat toiminnot toimialueen PDC:ssä

/SYNC

Toimialueen PDC:ssä annettuna tahdistaa toimialueen kaikkien palvelinten käyttäjätunnusasetukset PDC:n kanssa Palvelimella käytettynä tahdistaa kyseisen palvelimen käyttäjätietokannan toimialueen ohjauskoneen kanssa: komento koskee vain NT-koneita, jotka kuuluvat NT Server -toimialueeseen.

Esimerkiksi annetaan **NET ACCOUNTS /DOMAIN**-komento toimialueen PDC:ssä:

```
C:\>NET ACCOUNTS /DOMAIN
Force user logoff how long after time expires?:Never
Minimum password age (days):                   0
Maximum password age (days):                   Unlimited
Minimum password length:                       0
Length of password history maintained:         None
Lockout threshold:                             Never
Lockout duration (minutes):                    Never
Lockout observation window (minutes):          30
Computer role:                                 PRIMARY
The command completed successfully.
```

Huomataan, että mm. käyttäjätunnuksen lukitseminen ei ole käytössä.

NET GROUP

Lisää, näyttää tai muokkaa toimialueiden yleisiä ryhmiä (Global Group); komentoa voi käyttää vain Windows NT Server -toimialueilla.

Syntaksi:

NET GROUP [RYHMÄNIMI [/COMMENT:"TEKSTI"]] [/DOMAIN]
NET GROUP RYHMÄNIMI {/ADD [/COMMENT:"TEKSTI"] | /DELETE} [/DOMAIN]
NET GROUP RYHMÄNIMI KÄYTTÄJÄNIMI[...] {/ADD | /DELETE} [/DOMAIN]

Parametrit:

ei mitään Näyttää palvelimen ja sillä olevien ryhmien nimet

ryhmänimi Lisättävän, laajennettavan tai poistettavan ryhmän nimi. Jos **ryhmänimi** on ainoa annettu parametri, näyttöön tulee ryhmän jäsenluettelo

/COMMENT:"TEKSTI" Lisää kommentin uudelle tai jo olemassa olevalle ryhmälle; siinä voi olla enintään **48** merkkiä ja anna kommentti lainausmerkeissä

/DOMAIN	Suorittaa toiminnon toimialueen PDC:ssä; muussa tapauksessa toiminto suoritetaan paikallisessa työasemassa. Parametria käytetään vain niissä NT-tietokoneissa, jotka kuuluvat NT Server -toimialueeseen ja joihin **ei ole** asennettu NT Server -ohjelmistoa; oletusarvona NT Server -tietokoneet suorittavat toiminnot toimialueen PDC:ssä
KÄYTTÄJÄNIMI[...]	Yksi tai useampia käyttäjänimiä, jotka lisätään ryhmään tai poistetaan siitä; jos käyttäjänimiä on useampia kuin yksi, ne on erotettava toisistaan välilyönneillä
/ADD	Luo uuden ryhmän tai lisää käyttäjänimen ryhmään. Käyttäjätunnuksen on oltava luotuna ennen kuin se voidaan lisätä ryhmään tällä komennolla
/DELETE	Poistaa ryhmän tai käyttäjänimen ryhmästä.

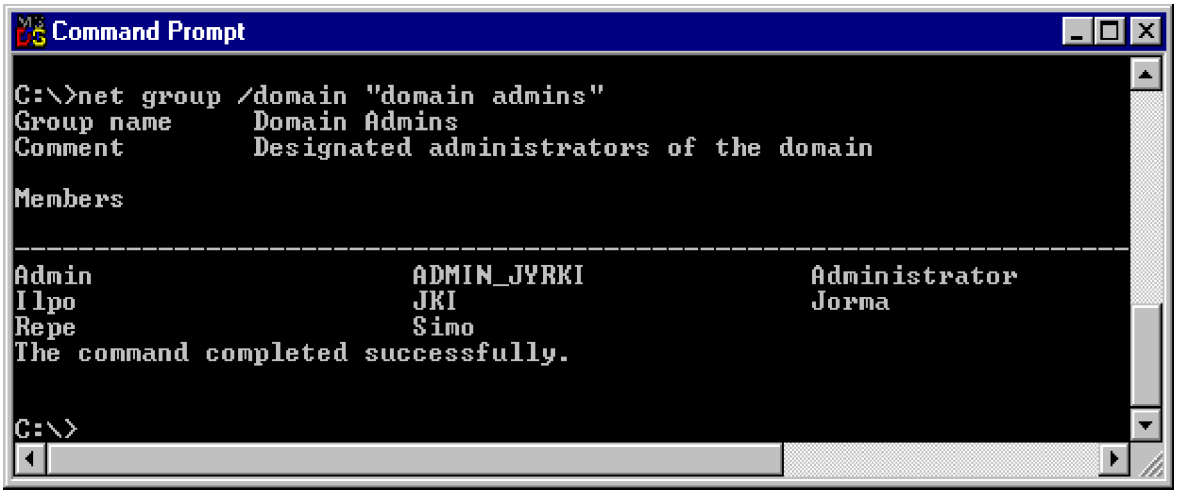
Esimerkkejä:

NET GROUP /DOMAIN

Esimerkkejä:

Domain Admins -ryhmän jäsenet:

NET GROUP "DOMAIN ADMINS"



Voit lisätä ryhmän **PCTuki** käyttäjätietokantaan palvelimella komennolla:

NET GROUP PCTUKI /ADD

Voit lisätä ryhmän **PCTuki** toimialueen käyttäjätietokantaan **työasemassa** komennolla:

NET GROUP PCTUKI /ADD /DOMAIN

Voit lisätä aikaisemmin luodut käyttäjätunnukset palvelimen ryhmään **PCTuki** komennolla:

NET GROUP PCTUKI JST ENI JIS JRI JKI AHA JJO /ADD

Voit lisätä aikaisemmin luodut käyttäjätunnukset toimialueen käyttäjätietokantaan **työaseman** komennolla:

NET GROUP PCTUKI JST ENI JIS JRI JKI AHA JJO /ADD /DOMAIN

Voit lisätä kommentin **PCTUKI**-ryhmän tietoihin komennolla:

NET GROUP PCTUKI /COMMENT:"All work and no play"

NET LOCALGROUP

Lisää, näyttää ja muokkaa **paikallisia ryhmiä** (Local Group).

Syntaksi:

NET LOCALGROUP [RYHMÄNIMI] [/DOMAIN]
NET LOCALGROUP RYHMÄNIMI {/ADD | /DELETE} [/DOMAIN]
NET LOCALGROUP RYHMÄNIMI NIMI [...] {/ADD | /DELETE} [/DOMAIN]

Parametrit:

ei mitään Näyttää toimialueen ja sillä olevien paikallisten ryhmien nimet

ryhmänimi Lisättävän, laajennettavan tai poistettavan ryhmän nimi. Jos ryhmänimi on ainoa annettu parametri, näyttöön tulee paikalliseen ryhmään kuuluvien käyttäjien ja yleisten ryhmien luettelo

/domain Suorittaa toiminnon toimialueen PDC:ssä; muussa tapauksessa toiminto suoritetaan **paikallisessa työasemassa**. Tätä parametria käytetään vain niissä NT-koneissa, jotka kuuluvat toimialueeseen ja jotka eivät ole ohjauskoneita; oletusarvona ohjaskoneet suorittavat toiminnot toimialueen PDC:ssä

nimi [...] Yksi tai useampia käyttäjä- tai ryhmänimiä, jotka lisätään paikalliseen ryhmään tai poistetaan siitä. Jos nimiä on useampia kuin yksi, ne on erotettava toisistaan välilyönneillä. Nimet voivat olla **paikallisia käyttäjiä**, muiden **toimialueiden käyttäjiä** tai **yleisiä ryh-**

miä, mutta **eivät paikallisia ryhmiä**. Jos käyttäjä on toisen toimialueen käyttäjä, kirjoita käyttäjänimen eteen toimialuenimi (esimerkiksi HALLINTO\ASKO)

/add Lisää **yleisen ryhmänimen** tai **käyttäjänimen paikalliseen ryhmään**. Käyttäjätunnuksen tai yleisen ryhmätunnuksen on oltava luotuna ennen kuin se voidaan lisätä paikalliseen ryhmään

/delete Poistaa **ryhmänimen** tai **käyttäjänimen** paikallisesta ryhmästä.

Esimerkki:

Komennot **VERSTAS**-toimialueen PDC:ssä:

NET LOCALGROUP

Voit lisätä paikallisen ryhmän **SPLAT** käyttäjätietokantaan palvelimella komennolla:

NET LOCALGROUP SPLAT /ADD

Voit lisätä aikaisemmin luodut käyttäjätunnukset toimialueen käyttäjätietokantaan komennolla:

NET LOCALGROUP SPLAT JST ENI JIS JRI JKI AHA JJO /ADD

NET USER

Lisää tai muokkaa tai näyttää käyttäjätunnuksia

NET USER [KÄYTTÄJÄ [SALASANA| *] [VALITSIMET]] [/DOMAIN]

NET USER KÄYTTÄJÄ {SALASANA | *} /ADD [VALITSIMET] [/DOMAIN]

NET USER KÄYTTÄJÄ [/DELETE] [/DOMAIN]

Parametrit:

ei mitään Näyttää palvelimen käyttäjätunnukset

KÄYTTÄJÄ Määrittää lisättävän, poistettavan, muokattavan tai näyttöön tuotavan käyttäjätunnuksen; siinä voi olla enintään **20** merkkiä

SALASANA Asettaa tai muuttaa käyttäjätunnuksen salasanan. Salasanassa on oltava **NET ACCOUNTS** -komennon **/MINPWLEN** -valitsimella määritetty vähimmäispituus; enimmäismäärä on **14** merkkiä

***** Salasana pyydetään kehotteella; salasana ei näy näytössä

/DOMAIN Suorittaa komennon toimialueen PDC:ssä; parametria käytetään vain niissä NT-koneissa, jotka kuuluvat toimialueeseen ja jotka eivät ole ohjauskoneita. Oletusarvona ohjauskoneet suorittavat toiminnot toimialueen PDC:ssä

/ADD Lisää käyttäjätunnuksen käyttäjätietokantaan

/DELETE Poistaa käyttäjätunnuksen käyttäjätietokannasta

Valitsimet ovat seuraavat:

/active:{no | yes} Ottaa käyttäjätilin käyttöön tai poistaa sen käytöstä - jos käyttäjätili **ei ole** aktiivinen, käyttäjä ei voi käyttää palvelimen resursseja. Oletusarvo on **yes** eli aktiivinen

/comment:"teksti" Käyttäjätunnusta kuvaava kommentti, jossa voi olla enintään **48** merkkiä ja teksti on kirjoitettava lainausmerkkeihin

/countrycode:nnn Käyttää käyttöjärjestelmän maakoodeja ohje- ja virheilmoitusten kielen määrittämiseen. Arvo **0** tarkoittaa maakoodin oletusarvoa; Suomi on **358**

/expires:{päivämäärä | never}
Määrittää käyttäjätunnuksen vanhenemaan päivämäärän ilmoittamana ajankohtana.- Vaihtoehto **never** poistaa aikarajoituksen. Vanhenemispäivämäärät annetaan **/countrycode** -asetuksen mukaan muodossa **pp.kk.vv**, **kkk.pp.vv** tai **kk/pp/vv**. Huomaa, että tunnus vanhenee määritetyn vanhenemispäivän alkaessa. Kuukausi voidaan antaa lukuna, kokonaan kirjoitettuna tai lyhennettynä. Vuosi voidaan antaa kaksi- tai nelinumeroisessa muodossa. Päivämäärän osat on erotettava toisistaan pisteillä tai vinoviivoilla - välilyöntejä ei saa käyttää. Jos vuosiosaa ei ole määritetty, päivämäärä tulkitaan seuraavaksi sopivaksi päiväksi

/fullname:"nimi" Määrittää käyttäjän koko nimen; teksti on kirjoitettava lainausmerkkeihin

/homedir:polku Määrittää käyttäjän kotihakemiston hakemistopolun ja sen on syytä olla olemassa

/passwordchg:{yes | no}	Määrittää, voivatko käyttäjät muuttaa omia salasanojaan. Oletusarvo on **yes** eli salasanoja voi muuttaa
/passwordreq:{yes | no}	Määrittää, onko käyttäjätunnuksilla oltava salasana. Oletusarvo on kyllä eli **yes**
/profilepath:[polku]	Määrittää käyttäjän profiilin hakemistopolun; **polku** osoittaa profiiliin
/scriptpath:polku	Määrittää käyttäjän kirjauskomentotiedoston (logon script) hakemistopolun. Polku ei voi olla absoluuttinen, vaan se on ilmoitettava polun **%systemroot%\SYSTEM32 \REPL\IMPORT\ SCRIPTS** suhteen
/times:{ajat | all}	Määrittää ajat, jolloin käyttäjä saa käyttää palvelinta; annettava muodossa **päivä[-päivä][,päivä[-päivä]],kellonaika[-kellonaika][,kellonaika[-kellonaika]],** missä kellonajat annetaan tunnin tarkkuudella. Päivien nimet voidaan kirjoittaa kokonaan tai lyhennetyssä muodossa, kellonajat voidaan antaa **12**- tai **24** tuntisessa muodossa. 12 tunnin muodossa on käytettävä merkintöjä **AM** ja **PM** tai **A.M.** ja **P.M.** erottamaan aamua ja iltaa toisistaan. Arvo **all** tarkoittaa, että käyttäjä voi kirjautua koska tahansa. **Tyhjä arvo tarkoittaa, että käyttäjä ei voi kirjautua lainkaan**. Päivä ja kellonaika on erotettava toisistaan pilkulla ja päivä-kellonaikaryhmät puolipisteellä. Välilyöntien käyttö ei ole sallittua
/usercomment:"teksti"	Muuttaa käyttäjätunnukselle määritettyä kommenttia; se on kirjoitettava lainausmerkkeihin

/workstations:{tietokonenimi[,...] | *}

Määrittää työasemat, joilta käyttäjä saa kirjautua verkkoon; työasemia voi olla enintään kahdeksan ja ne on erotettava toisistaan pilkuilla. Jos **/workstations** -valitsimella ei ole määritetty työasemaluetteloa tai jos määritetty arvo on *****, käyttäjä voi kirjautua miltä tahansa työasemalta.

Esimerkkejä:

Lisätään käyttäjätunnus **BJORN** ilman salasanaa, profiilin asetuksilla:

C:\>NET USER BJORN /HOMEDIR:\\V1\USERS\BJORN /PROFILEPATH:\\V1\USERS\BJORN

Ole varovainen **NET USER**-komennon yhteydessä **%USERNAME%**-muuttujan kanssa; sen arvo on kirjautuneen käyttäjän, jos muuta ei aseteta.

Poistetaan käyttäjätunnus **SIPA**:

C:\>NET USER SIPA /DELETE

Käyttäjätunnusten luominen komentojonolla

Yhdistelemällä komentojonoja ja NET-komentoja on helppo ylläpitää melkoista määrää käyttäjätunnuksia.

Halutaan lisätä kerralla suuri joukko toimialueen käyttäjiä, joille määritellään kotihakemistoksi palvelimen **V1** jakamasta hakemistosta käyttäjätunnuksen mukainen hakemisto.

Halutaan lisäksi käyttäjälle palvelimella sijaitseva profiili (Roaming profile) sekä suojata profiilihakemisto. Lisäksi halutaan luoda ja suojata myös kotihakemisto.

Käytetään hyväksi NT:n **CACLS**- ja **NET USER**-komentoja. Tehdään ensin komentojono **ADDUSERS.BAT**:

```
MD \\V2\USERS\%1
NET USER %1 %2 /ADD /DOMAIN /FULLNAME:"%3" /COUNTRYCODE:358 /EXPIRES:NEVER /PASSWORDCHG:NO /PROFILEPATH:\\V2\Profiles\%1 /HOMEDIR:\\V2\USERS\%1
CACLS \\V2\USERS\%1 /E /G %1:F
CACLS \\V2\USERS\%1 /E /R Everyone
```

Komentojono tekee seuraavaa:

- Luo kotihakemiston (**MD \\V2\USERS\%1**)
- Lisää käyttäjän **Domain Users**-ryhmään ja määrittelee koko nimen (**/FULLNAME**)
- Kytkee automaattisesti **Z:**-aseman käyttäjän kotihakemistoon (**/HOMEDIR:\\V2\USERS\%1**)
- Luo käyttäjälle palvelimella sijaitsevan profiilin (*Roaming*) (**/PROFILEPATH:\\V2\Profiles\%1**)
- Salasana ei vanhene (**/EXPIRES:NEVER**) eikä salasanaa ei voi muuttaa (**/PASSWORDCHG:NO**)
- Antaa käyttäjälle täydet oikeudet kotihakemistoon (**CACLS \\V2\USERS\%1 /E /G %1:F**)
- Poistaa **Everyone**-ryhmältä oikeudet kotihakemistoon (**CACLS \\V2\USERS\%1 /E /R Everyone**).

Komentorivin komennolla

ADDUSERS JTO salasana "TORRANCE,JACK"

voidaan nyt lisätä käyttäjätunnus **JACKT**, jonka salasana on **salasana** ja nimi **TORRANCE,JACK**.

Nyt tehdään lisäksi **USERS.BAT**, johon lisätään rivi jokaiselle luotavalle käyttäjälle; tällaisen tekee helposti sopivalla editorilla tai vaikkapa Excelillä:

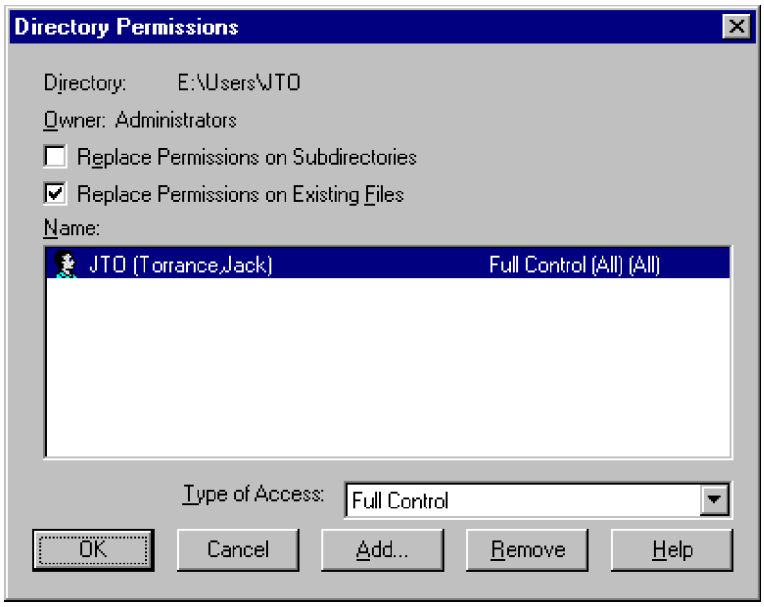
```
CALL ADDUSERS JTO salasana "Torrance,Jack"
CALL ADDUSERS STE salasana "Templar,Simon"
CALL ADDUSERS KWA salasana "Walker,Kit"
CALL ADDUSERS PKI salasana "Kimble,Paul"
CALL ADDUSERS NSO salasana "Solo,Napoleon"
CALL ADDUSERS BWA salasana "Wayne,Bruce"
CALL ADDUSERS HLE salasana "Lecter,Hannibal"
```

Tämän jälkeen annetaan komentorivin komento

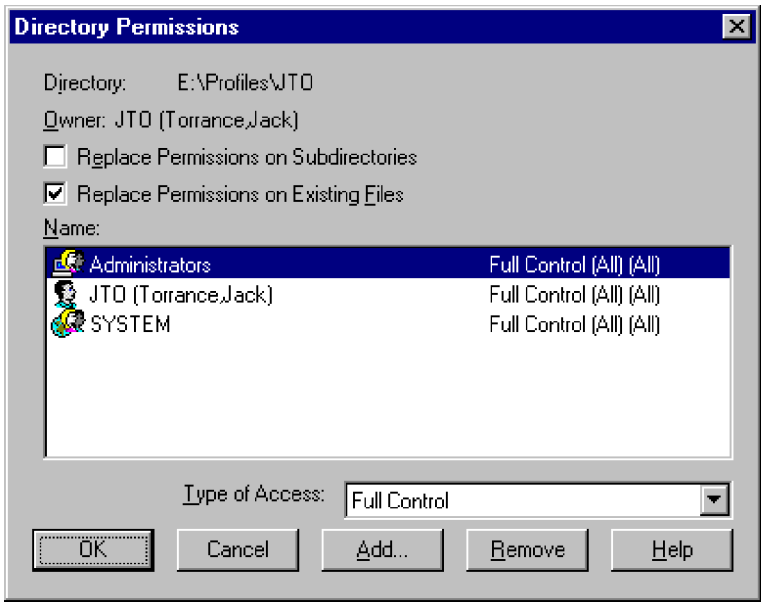
USERS

ja käyttäjät luodaan.

Kun käyttäjä kirjautuu toimialueelle, hän saa käyttöönsä palvelimella sijaitsevan profiilin ja kotihakemiston. Kotihakemistoon on vain käyttäjällä oikeus:



Profiilin hakemistoon on seuraavat oikeudet:



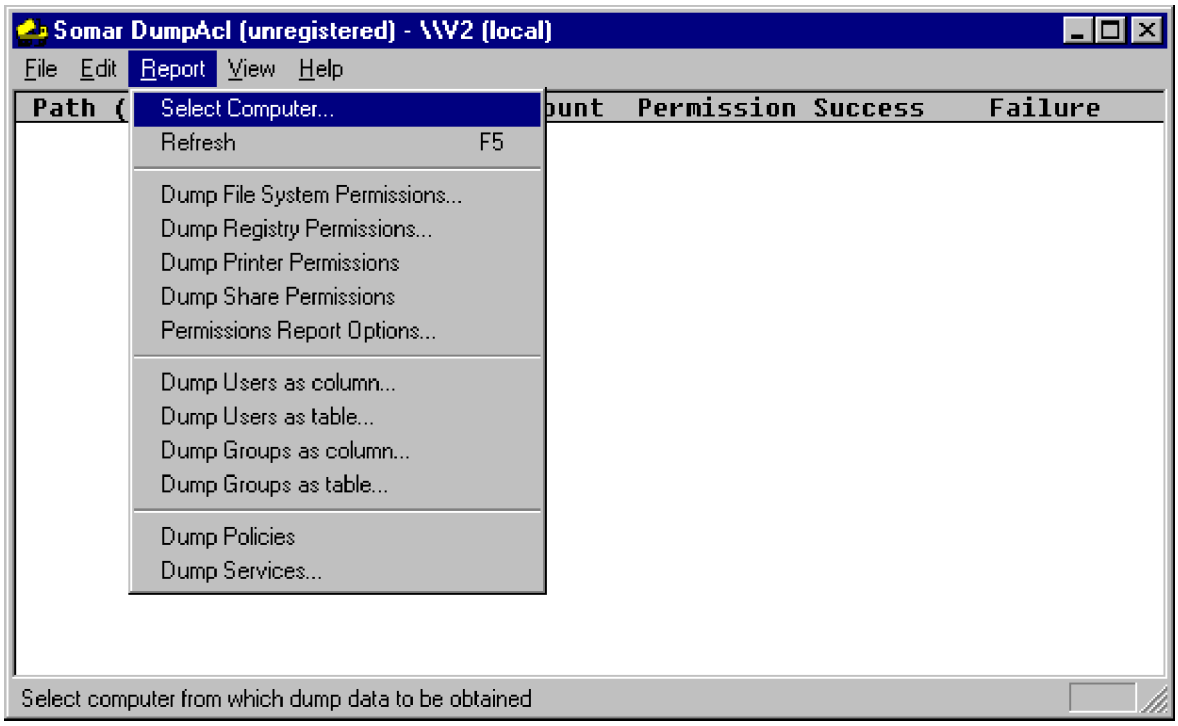
Apuohjelmia käyttäjien hallintaan

Seuraavaksi käsitellään muita kuin Windows NT:n mukana tulevia työkaluja käyttäjien hallintaan.

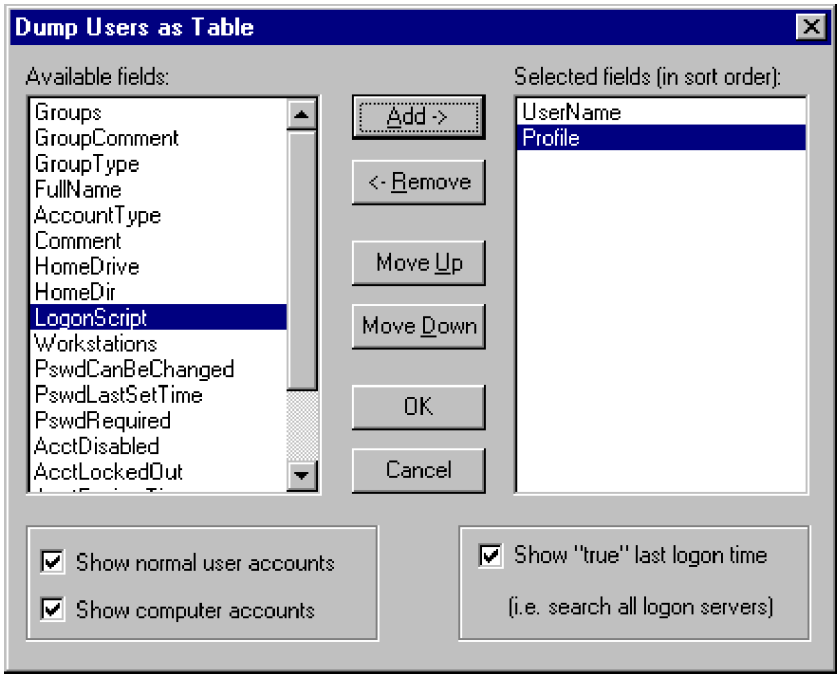
SomarSoftin (**http://www.somar.com**) **DumpACL**:ää lukuunottamatta kyseessä on **Windows NT 4.0 Resource Kit**in mukana tulevia työkaluja.

DUMPACL

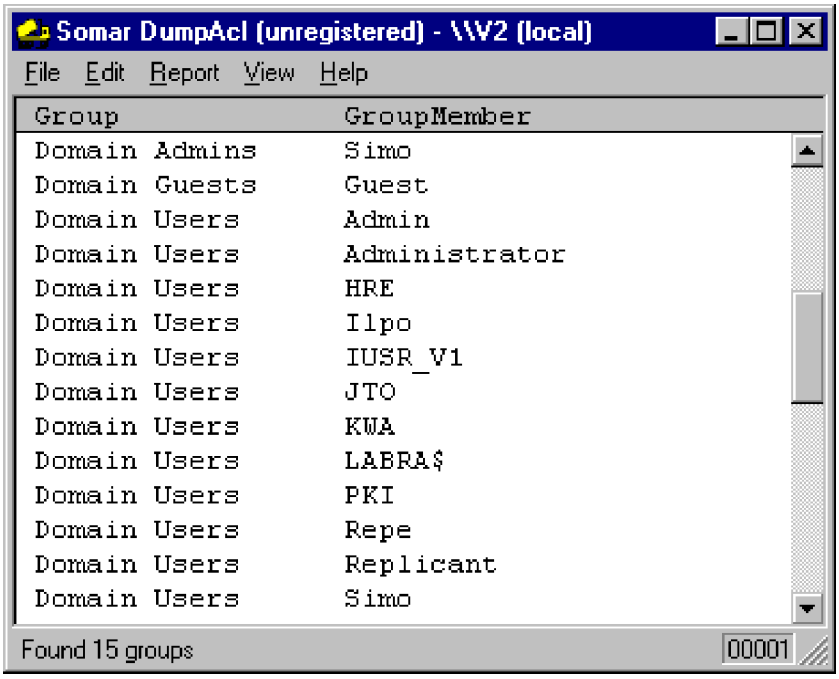
DumpACL on **SomarSoftin** apuohjelma käyttäjien, käyttäjäryhmien, käyttöoikeusluetteloiden jne tarkasteluun. Käyttäjiä tai käyttäjien asetuksia tällä ei voi muuttaa, mutta raportit ovat sitäkin parempia. Internetistä (**http://www.somar.com**) voi imuroida kokeiluversion.



Käyttäjien listauksessa voidaan valita halutut tiedot...



Ja käyttäjäryhmien listaukset ovat erittäin helppolukuisia! Suosittelen.



ADDUSERS

ADDUSERS.EXE on apuohjelma, jolla voit hallita käyttäjiä määrämuotoisen tekstitiedoston avulla.

Syntaksi on:

ADDUSERS [/?] [\\NT-kone [[/c | /d | /e] tdostonimi]] [/s:?]

Parametrit ovat:

/?	Opaste
/c	Luo käyttäjätunnukset
/d	Listaus käyttäjätunnuksista tiedostoon
/e	Poista määritelty käyttäjätunnus
/s:?	Syöttö/tulostustiedoston erotinmerkki, oletus on **,**

NT-kone kohdekone

Huomaa:

- Käyttäjätunnuksen poistaminen poistaa myös SID:n
- Listaus ei sisällä käyttäjätunnusta.

Ohjaustiedoston syntaksi on:

[User]
<User Name>,<Full Name>,<Password>,<Home Drive>,<Home Path>,<Profile>,<Script>
[Global]
<Global Group Name>,<Comment>,<UserName>, ...
[Local]
<Local Group Name>,<Comment>,<UserName>, ...

Huomaa, että ryhmät määritellään sektioissa **Users**, **Global** ja **Local**.

Helpoimmalla pääset, kun luot ensin tulostustiedoston ja käytät sitä mallina.

Esimerkkejä:

C:\ADDUSERS /D LISTA.TXT

Luo tiedoston **LISTA.TXT**, jonka alkuosa:

```
[User]
Admin,,,,,,,
Administrator,,,Built-in account for administering the compu-
ter/domain,,,,
Guest,,,Built-in account for guest access to the computer/domain,,,,
IUSR_V1,Internet Guest Account,,Internet Server Anonymous Access,,,,
JTO,Torrance,Jack,,,,\\V2\USERS\JTO,\\V2\Profiles\JTO,
KWA,Walker,Kit,,,,\\V2\USERS\KWA,\\V2\Profiles\KWA,
PKI,Kimble,Paul,,,,\\V2\USERS\PKI,\\V2\Profiles\PKI,
SQLExecutiveCmdExec,SQLExecutiveCmdExec,,SQL Executive CmdE-
xec Task Account,,D:\,,
STE,Templar,Simon,,,,\\V2\USERS\STE,\\V2\Profiles\STE,
[Global]
Domain Admins,Designated administrators of the domain,Administrator,
Domain Guests,All domain guests,Guest,
```

Luodaan käyttäjätunnus ohjaustiedostosta **HRE.TXT**, joka näyttää tältä:

```
[User]
HRE,Recknagel Helmut,,,,\\V2\USERS\HRE,\\V2\Profiles\HRE,
```

Komento on:

```
C:\>ADDUSERS /C \HRE.TXT
User account created:  "HRE"
  - Home directory created:  "\\V2\USERS\HRE"
```

GETSID

GETSID.EXE vertailee käyttäjätunnuksen SID:iä (*Security Identifier*). Tällä voidaan todeta esimerkiksi käyttäjätietokannan korruptoituminen.

Syntaksi on:

GETSID \\NT-kone1 käyttäjätunnus \\NT-kone2 käyttäjätunnus

Esimerkiksi

```
C:\>GETSID \\V1 JKI  \\V5 JKI
The SID for account VERSTAS\JKI matches account VERSTAS\JKI
The SID for account VERSTAS\JKI is
S-1-5-21-1289181413-810293876-390482200-1002
The SID for account VERSTAS\JKI is
S-1-5-21-1289181413-810293876-390482200-1002
```

SID käyttäjätunnukselle **JKI** on sama PDC:n (**V1**) ja BDC:n (**V5**) välillä, eli asiat ovat kunnossa tältä osin.

GLOBAL

GLOBAL.EXE näyttää yleisten käyttäjäryhmien (*Global group*) jäsenet kohteessa.

Syntaksi on:

GLOBAL ryhmä toimialue| \\NT-kone

Parametrit:

ryhmä	Kysyttävä yleinen ryhmä
toimialue	Toimialueen nimi
NT-kone	Kohdepalvelimen nimi

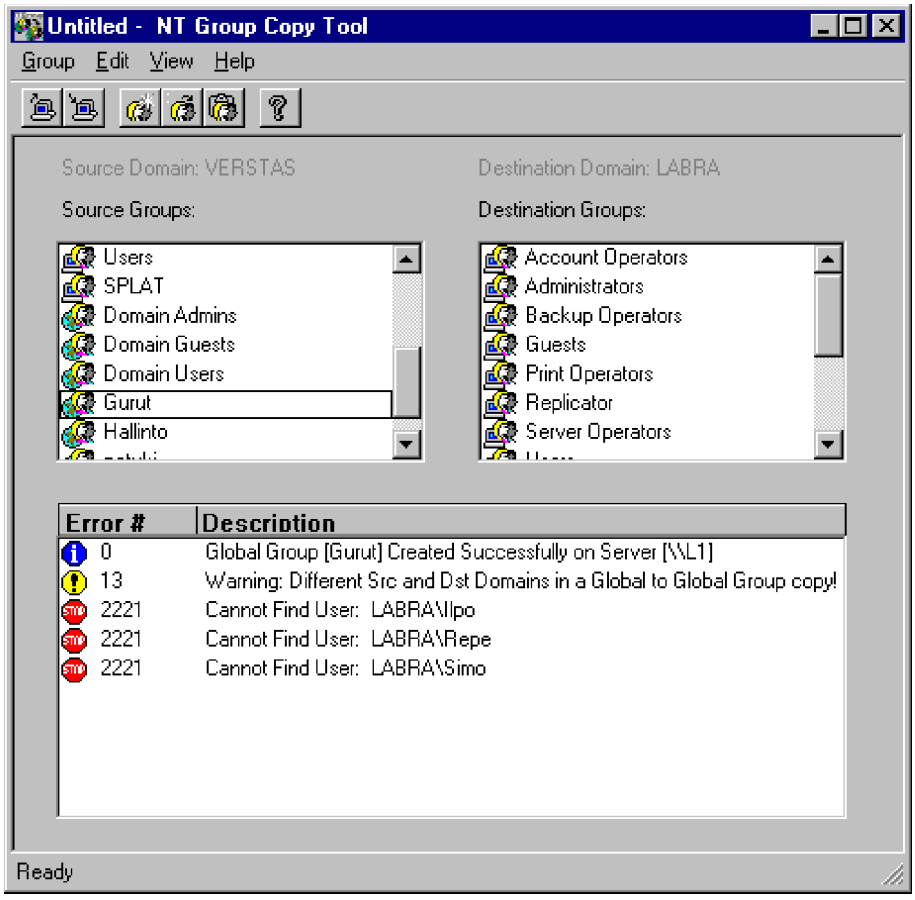
Esimerkiksi yleisen ryhmän **Domain Users** jäsenet toimialueella **VERSTAS**:

```
C:\>GLOBAL "Domain Users" VERSTAS
Administrator
V1$
Admin
V2$
IUSR_V1
V3$
SQLExecutiveCmdExec
V4$
Template
LABRA$
WS1$
WS2$
WS3$
WS4$
WS5$
WS6$
Replicant
```

Huomaa, että näet myös luottavan toimialueen nimen (**LABRA$**) sekä toimialueen konetunnukset (esimerkiksi **WS1$**).

GRPCPY

GRPCPY.EXE mahdollistaa käyttäjäryhmien kopioimisen toimialueelta toiseen tai saman toimialueen sisällä. Käyttäjätunnusten on oltava olemassa kohdetoimialueella.



Valikot ovat:

Group:

Set Source Domain Asettaa lähdetoimialueen

Set Destination Domain Asettaa kohdetoimialueen

Edit:

Copy to New Group Kopioi kohteessa uuteen ryhmään

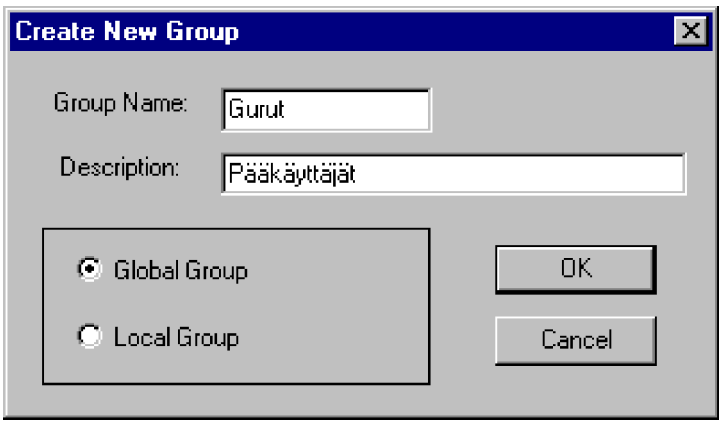
Copy to Destination	Kopioi kohteeseen sellaisenaan
Copy from Clipboard	Kopioi leikepöydältä.

Esimerkiksi kopioidaan ryhmä **Gurut** toimialueelta toiseen. Toimitaan seuraavasti:

1) Valitse **Group** | **Set Source Domain** ja aseta lähdetoimialue

2) Valitse **Group** | **Set Destination Domain** ja aseta kohdetoimialue

3) Valitse lähderyhmä ja valitse **Edit** | **Copy to New Group**



4) Annetaan ryhmän nimi kohteessa

5) Painetaan **OK**.

Esimerkiksi kopioidaan ryhmän **Gurut** jäsenyydet toimialueelta toiseen. Toimitaan seuraavasti:

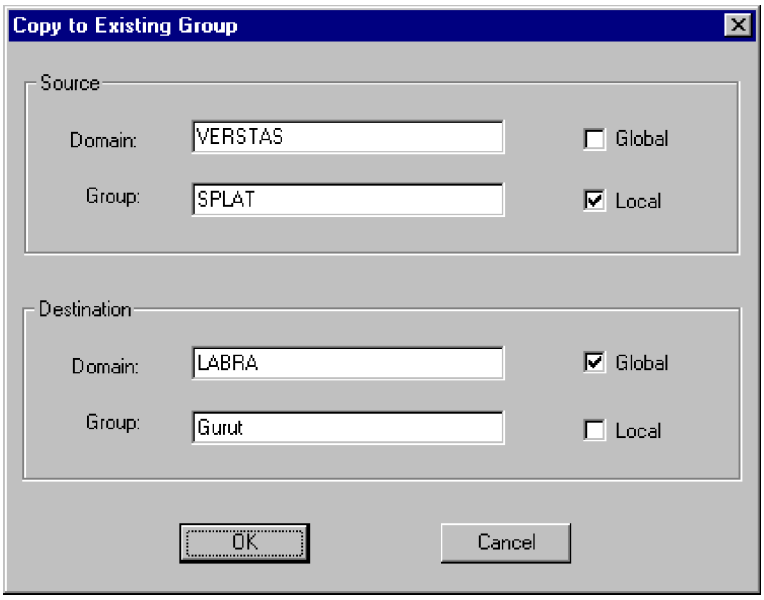
1) Valitse **Group** | **Set Source Domain** ja aseta lähdetoimialue

2) Valitse **Group** | **Set Destination Domain** ja aseta kohdetoimialue

3) Valitse lähderyhmä

4) Valitse kohderyhmä

5) ja valitse **Edit** | **Copy to Destination**



5) Painetaan **OK**.

Listan tapahtumista näet ikkunan alaosassa.

IFMEMBER

IFMEMBER.EXE tutkii kirjautuneen käyttäjän ryhmäjäsenyydet.

Syntaksi on:

IFMEMBER [/V] [/L] ryhmä

Parametrit:

/V Tarkistaa, kuuluuko käyttäjä kyseiseen ryhmään
/L Listaa kaikki ryhmät, joihin käyttäjä kuuluu

Esimerkkejä - onko kirjautunut käyttäjä **Domain Users**-ryhmässä ja mihin ryhmiin käyttäjä kuuluu:

```
C:\>IFMEMBER /V /L "Domain Users"
User is a member of group VERSTAS\Domain Users.
Group VERSTAS\Domain Users matches list.
User is a member of group \Everyone.
User is a member of group BUILTIN\Administrators.
```

```
User is a member of group BUILTIN\Users.
User is a member of group VERSTAS\Domain Admins.
User is a member of group \LOCAL.
User is a member of group NT AUTHORITY\INTERACTIVE.
User is a member of group NT AUTHORITY\Authenticated Users.
```

Paluukoodia **errorlevel** voi käyttää hyväksi. Arvo **1** pitää paikkansa, eli käyttäjä kuuluu ryhmään:

```
ifmember Administrators
if not errorlevel 1 exit
NET USE X: /D
NET USE X: \\V1\PCTUKI
```

Tässä esimerkissä komentojonon kaksi viimeistä riviä ajetaan vain, jos käyttäjä kuuluu **Administrators**-ryhmään.

LOCAL

LOCAL.EXE näyttää paikallisten käyttäjäryhmien (*Lobal group*) jäsenet kohteessa.

Syntaksi on:

```
LOCAL ryhmä toimialue| \\NT-kone
```

Parametrit:

ryhmä Kysyttävä yleinen ryhmä
toimialue Toimialueen nimi
NT-kone Kohdepalvelimen nimi

Esimerkiksi ryhmän **Users** jäsenet toimialueella **LABRA**:

```
C:\>LOCAL Users LABRA
Domain Users
SQLExecutiveCmdExec
```

SHOWGRPS

SHOWGRPS.EXE näyttää käyttäjän ryhmäjäsenyydet kohteessa.

Syntaksi on:

SHOWGRPS toimialue\käyttäjätunnus | käyttäjätunnus

Esimerkiksi **LABRA**-toimialueen käyttäjätunnuksen **JKI** ryhmäjäsenyydet:

```
C:\>SHOWGRPS LABRA\JKI

User: [LABRA\JKI], is a member of:

  BUILTIN\Administrators
  LABRA\Domain Admins
  LABRA\Domain Users
  \Everyone
  LABRA\Gurut
  LABRA\SPLAt2
```

SHOWMBRS

SHOWMBRS.EXE näyttää ryhmän käyttäjätunnukset.

Syntaksi on:

SHOWMBRS toimialue\käyttäjätunnus | käyttäjätunnus

Esimerkiksi **LABRA**-toimialueen **Domain Users**-ryhmän jäsenet:

```
C:\>SHOWMBRS  "LABRA\Domain Users"

Members of global group [LABRA\Domain Users]:

  JKI
  L1$
  IUSR_L1
  SQLExecutiveCmdExec
  Admin
```

SRVCHECK

SRVCHECK.EXE listaa valitun palvelimen jakonimet ja niiden oikeudet.

Syntaksi on:

SRVCHECK \\NT-kone

Esimerkiksi **palvelimen V4** jaot ja käyttäjien oikeudet:

```
C:\> SRVCHECK \\V4
\\v2\NETLOGON
   .\Everyone
\\v2\Asennus
\\v2\HPLaserJ
   BUILTIN/Server Operators
   BUILTIN/Print Operators
   BUILTIN/Administrators
            VERSTAS/Administrator
            VERSTAS/Domain Admins
            VERSTAS/Admin
            VERSTAS/JKI
            VERSTAS/Repe
            VERSTAS/Ilpo
            VERSTAS/Simo
   .\Everyone
\\v2\REPL$
   BUILTIN/Administrators
            VERSTAS/Administrator
            VERSTAS/Domain Admins
            VERSTAS/Admin
            VERSTAS/JKI
            VERSTAS/Repe
            VERSTAS/Ilpo
            VERSTAS/Simo
   BUILTIN/Replicator
            VERSTAS/Replicant
```

jne

USRSTAT

USRSTAT.EXE näyttää käyttäjätunnuksen, käyttäjän nimen ja edellisen kirjautumisajankohdan.

Syntaksi on:

USRSTAT toimialue

Esimerkiksi kirjautumisajat **VERSTAS**-toimialueella:

```
C:\> USRSTAT VERSTAS
Users at \\V1
Admin -                          - logon: Thu Jun 05 18:45:28 1997
Administrator -                  - logon: Thu Jun 05 15:32:19 1997
Guest -                          - logon:          Never
HRE -        Recknagel Helmut    - logon: Thu Jun 05 15:44:24 1997
IUSR_V1 -    Internet Guest Account - logon: Thu Jun 05 15:45:28 1997
JTO -        Torrance,Jack       - logon: Thu Jun 05 17:40:10 1997
KWA -        Walker,Kit          - logon: Thu Jun 05 14:12:18 1997
PKI -        Kimble,Paul         - logon: Thu Jun 05 15:42:28 1997
STE -        Templar,Simon       - logon: Thu Jun 05 05:15:22 1997
Replicant -                      - logon: Thu Jun 05 15:34:35 1997

Users at \\V2
Admin -                          - logon: Thu Jun 05 18:45:28 1997
Administrator -                  - logon: Thu Jun 05 15:32:19 1997
Guest -                          - logon:          Never
HRE -        Recknagel Helmut    - logon: Thu Jun 05 15:44:24 1997
IUSR_V1 -    Internet Guest Account - logon: Thu Jun 05 15:45:28 1997
JTO -        Torrance,Jack       - logon: Thu Jun 05 17:40:10 1997
KWA -        Walker,Kit          - logon: Thu Jun 05 14:12:18 1997
PKI -        Kimble,Paul         - logon: Thu Jun 05 15:42:28 1997
STE -        Templar,Simon       - logon: Thu Jun 05 05:15:22 1997
Replicant -                      - logon: Thu Jun 05 15:34:35 1997
```

USRTOGRP

Komennon avulla voi lisätä käyttäjiä ryhmiin tekstitiedostosta. Ryhmä ja käyttäjätunnukset on oltava olemassa.

Syntaksi on:

USRTOGRP tekstitiedosto

Tekstitiedoston syntaksi on:

```
DOMAIN: toimialue
LOCALGROUP: paikallinen käyttäjäryhmä
Käyttäjätunnus1
Käyttäjätunnus2
Käyttäjätunnus3
jne
```

Esimerkiksi lisätään käyttäjiä tekstitiedostosta **L.TXT**:

```
DOMAIN: VERSTAS
LOCALGROUP: Users
STE
HLE
```

Komento on:

```
C:\>USRTOGRP L.TXT

Domain name: VERSTAS
Local group: Users
The "Users" group already exists on the VERSTAS domain.

Processing user names...
User:VERSTAS\STE                Status: successfully added.
User:(null)\HLE                 Status: no such user.
```

Huomaa, että käyttäjää **HLE** ei lisätty koska sitä ei ollut!

Käyttäjäprofiilit

Windows NT 4.0 mahdollistaa käyttäjäprofiilit, jolloin käyttäjän työskentely-ympäristö pystytään tarvittaessa tallentamaan palvelimelle; tällöin käyttäjä saa miltä tahansa Windows NT 4.0 -työasemalta oman työskentely-ympäristönsä käyttöönsä.

Windows NT 4.0:ssa jokaisen käyttäjän ympäristö tallennetaan **profiiliin**. Se voi lisäksi olla käyttäjä- tai ryhmäkohtainen ja sen voi tarvittaessa poistaa. Profiilin tyyppi voi olla:

- **Paikallinen** (Local)
- **Palvelimella**(Roaming)
- **Pakollinen** (Mandatory)

Huomattavaa:

- Windows 95:n ja Windows NT 3.51:n käyttäjäprofiilit eivät ole yhteensopivia Windows NT 4.0:n käyttäjäprofiilien kanssa, mutta niitä voi käyttää rinnakkain. Jos käyttäjä kirjautuu eri käyttöjärjestelmien työasemista toimialueelle, muutokset eivät siis päivity toisten käyttöjärjestelmien profiileihin.
- Windows NT 4.0-työasemien käyttäjien profiilit toimivat myös aiemmissa Windows NT-palvelinverkoissa.
- Suomenkielinen Windows NT 4.0 ja englanninkielinen Windows NT 4.0 käyttää eri profiilia, koska hakemistojen nimet eroavat.
- Käytettäessä palvelimella sijatisevaa profiilia palvelimen versio voi olla mikä tahansa, vaikkapa **3.50** tai **3.51**.
- Jos sekä Windows NT 4.0-työaseman **paikallinen käyttäjätunnus** että Windows NT-toimialueella määritelty käyttäjätunnus on sama, niin työaseman hakemistorakenteeseen tulee kaksi käyttäjätunnuksen mukaista hakemistoa, esimerkiksi **JKI** ja **JKI.000**.

Profiilin rakenne

Käyttäjän profiili sisältää kaksi osaa:

1) Järjestelmäkansiot (*folder*), jotka sijaitsevat **Profiles**-järjestelmähakemistossa (**\%Systemroot%\Profiles**, esimerkiksi työasemassa **C:\Winnt\Profiles**). Alihakemistoista tärkeimpiä voi käsitellä tarvittaessa suoraan **Käynnistä** (Start)-valikosta. Suomenkielinen Windows NT 4.0 ja englanninkielinen Windows NT 4.0 käyttää eri profiilia, koska hakemistojen nimet eroavat:

Kansio (US)	Kansio (FIN)	Merkitys
Application Data	**Sovellustiedot**	Esimerkiksi käyttäjäkohtainen sanasto
Desktop	**Työpöytä**	Käyttäjän työpöytä
Favorites	**Omat asetukset**	Pikakuvakkeet esim. Internetin osoitteisiin (Internet Explorer tukee)
NetHood	**Verkkoympäristö**	Verkkoympäristön pikakuvakkeet, jotka halutaan Network Neighborhood-ikkunaan
Personal	**Henkilökohtainen**	Pikakuvakkeet sovellusten kohteisiin
PrintHood	**Kirjoitinympäristö**	Pikakuvakkeet Printers-ikkunaan
Recent	**Recent**	Pikakuvakkeet viimeksi käsiteltyihin tiedostoihin
SendTo	**SendTo**	Hiiren pikavalikon Lähetä-valinta
StartMenu	**Käynnistä-valikko**	Käynnistysvalikko
Templates	**Mallit**	Mallitiedostot

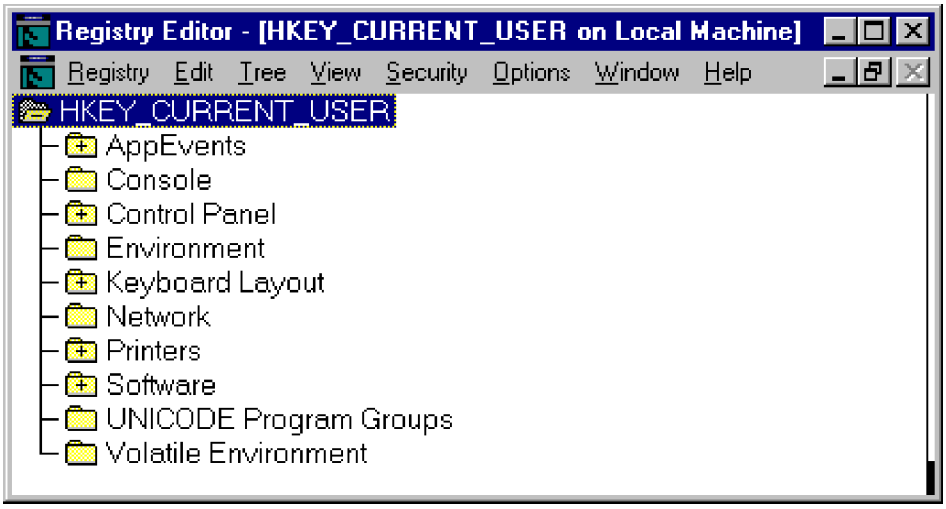
Jos sekä Windows NT -työaseman **paikallinen käyttäjätunnus** että Windows NT -toimialueella määritelty käyttäjätunnus on sama, niin työaseman hakemistorakenteeseen tulee kaksi käyttäjätunnuksen mukaista hakemistoa, esimerkiksi **JKI** ja **JKI.000**.

2) Tiedosto **NTUser.dat** on käyttäjätunnuksen mukaisessa **Profiles**-järjestelmähakemiston alihakemistossa. Profiiliitiedostoon **NTUser.dat** tallennetaan seuraavat asetukset:

- **Resurssienhallinta** (Explorer)
- **Tehtäväpalkki** (Taskbar)
- **Kirjoittimen** asetukset
- **Ohjauspaneeli** (Control Panel)
- **Apuohjelmien** asetuksia
- **Opasteen** kirjanmerkit.

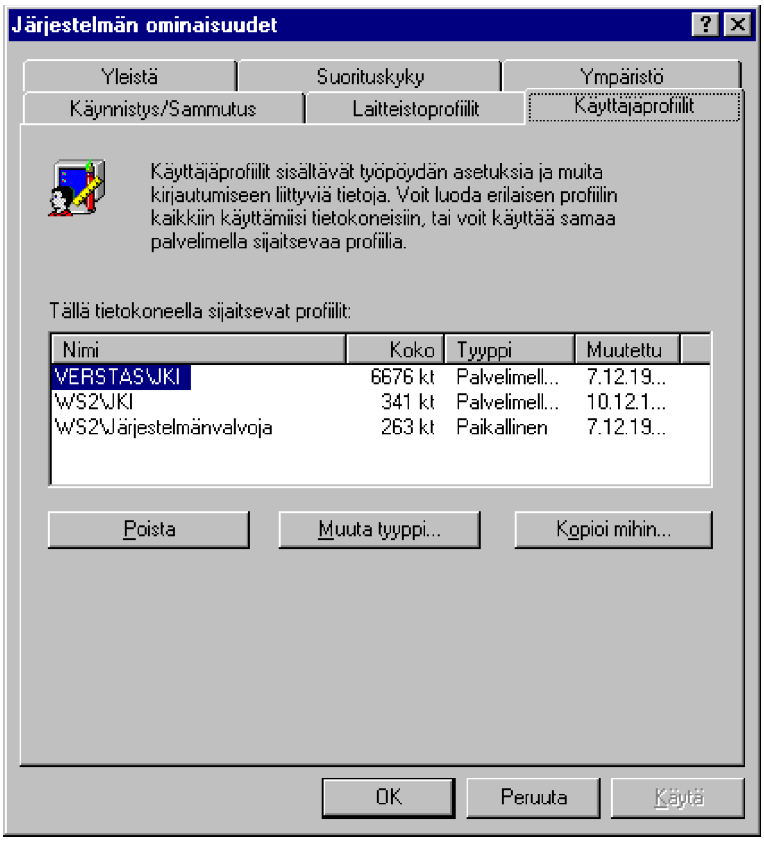
Profiiliitiedoston tiedostonimi voi olla henkilökohtaisen profiilin (**NTUser.dat**) tai pakollisen käyttäjäprofiilin (**NTUser.man**) nimi. Tiedosto **Ntuser.dat.log** sisältää rekisterin muutostapahtumat.

Profiiliitiedosto **NTUser.dat** on itseasiassa rekisterin osa **HKEY_CURRENT_USER**.



Käyttäjäprofiilien hallinta

Windows NT 4.0 -työasemassa tai -palvelimessa **aiemmin** kirjautuneiden käyttäjien profiilit tyyppeineen näet **Järjestelmä** (System)-kuvakkeen **Käyttäjäprofiilit** (User Profiles)-välilehdessä.



Jos sekä Windows NT -työaseman **paikallinen käyttäjätunnus** että Windows NT -toimialueella määritelty käyttäjätunnus on sama, niin työaseman hakemistorakenteeseen tulee kaksi käyttäjätunnuksen mukaista hakemistoa, esimerkiksi **JKI** ja **JKI.000**.

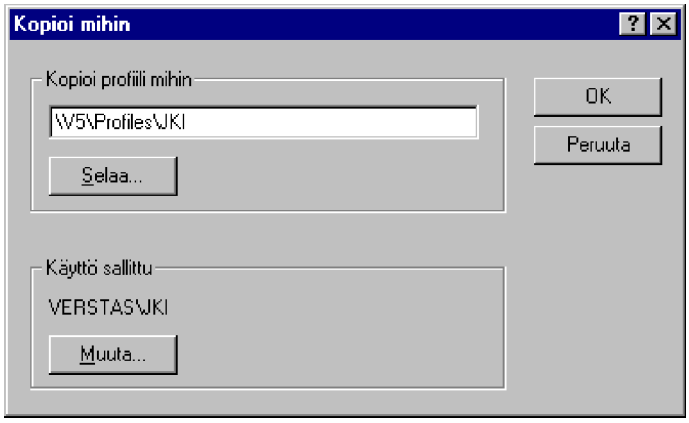
Käyttäjän profiili voi olla **paikallinen** (*Local*), eli sijaita vain NT-työaseman paikallisessa **Profiles**-järjestelmähakemistossa tai **palvelimella sijaitseva** (*Roaming*).

Jos haluat määritellä käyttäjälle **palvelimella sijaitsevan** (*Roaming*) profiilin, määritä käyttäjäprofiilin sijainti kirjoittamalla sen polku **User Manager for Domainsilla** käyttäjän profiilin asetuksissa **User Profile Path**-ruutuun; polun on oltava **verkkopolku** annettuna UNC-nimellä, esimerkiksi **\\V1\PROFILES\JKI**.

Lisäksi mahdollisen työasemassa jo sijaitseva **paikallisen** (*Local*) profiilin tyyppi ja sijainti on muutettava. Käyttäjän profiilin sijaintia **et** kuitenkaan voi muuttaa esimerkiksi **Resurssienhallinnalla** (Explorer). Sen sijaan työaseman **Käyttäjäprofiilit** (User Profiles)-välilehdessä **Muuta tyyppi** (Change Type)- ja **Kopioi mihin** (Copy To)-painikkeilla voit muuttaa profiilin tyyppiä ja sijaintia.

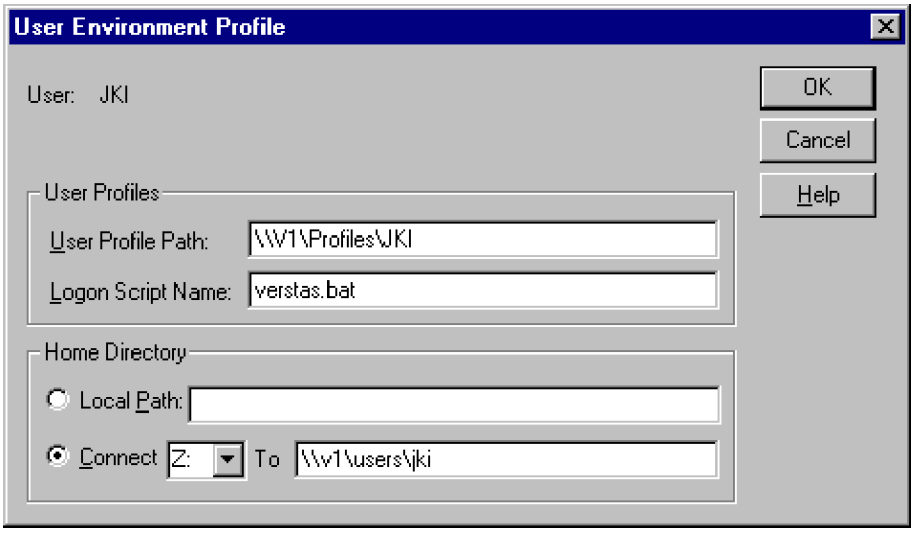
Tätä menettelyä kannattaa käyttää, jos käyttäjällä on jo työasemassaan toimiva työskentely-ympäristö ja siitä halutaan tehdä **palvelimella sijaitseva** (*Roaming*) profiili. Valitse profiili, paina **Kopioi mihin** (Copy To)-painiketta ja valitse kohteeksi käyttäjän palvelimella sijaitseva profiilin hakemisto - sama mikä on käyttäjälle annettu **Käyttäjien hallinnassa** (User Manager) tai **User Manager for Domainsissa**. Anna myös käyttäjille oikeudet **Muuta** (Change)-painikkeella käyttää a.o. profiilia.

Voit myös **Poistaa** (Delete) profiilin, jos et ole tällä hetkellä kirjautunut käyttäjätunnuksella, joka käyttää a.o. profiilia.



Palvelimella sijaitseva profiili

Jos haluat määritellä käyttäjälle **palvelimella sijaitsevan** (*Roaming*) profiilin, määritä käyttäjäprofiilin sijainti **User Manager for Domains**issa kirjoittamalla sen polku profiilin asetuksissa **Käyttäjäprofiilin polku** (User Profile Path) -ruutuun; polun on oltava **verkkopolku** annettuna UNC-nimellä, esimerkiksi **\\V1\PROFILES\JKI**.



Lisäksi mahdollisen työasemassa jo sijaitseva **paikallisen** (*Local*) profiilin tyyppi ja sijainti on muutettava on **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen avulla. **Käyttäjäprofiilit** (User Profiles)-välilehden **Muuta tyyppi** (Change Type)- ja **Kopioi mihin** (Copy To)-painikkeilla voit muuttaa profiilin tyyppiä ja sijaintia.

Tarkista, että käyttäjällä on profiilihakemistoonsa riittävät oikeudet:

- **Kirjoitusoikeudet**, jos käyttäjä saa muuttaa profiiliaan
- **Lukuoikeudet**, jos käyttäjän profiili on jo olemassa.

Profiili kuitenkin kopioidaan ensin työaseman kiintolevylle, josta sitä käytetään. Vasta kun käyttäjä kirjautuu pois toimialueelta, profiili päivitetään palvelimelle.

Profiili jää kiintolevylle, jos sitä ei erikseen poisteta rekisterin asetuksella (ks. myös Policy Editor).

Jos käyttäjän kirjautumisen yhteydessä palvelimella sijaitsevaan profiiliin ei päästä käsiksi (tai kyseessä on hidas linkki), kysytään, käytetäänkö palvelimella sijaitsevaa vai paikallista profiilia (joka saattaa olla vanhempi).

Profiiliin liittyy eräs tietoturvallisuusriski. Jos käyttäjä tallentaa työpöydälleen työtiedostojaan, niin kuka tahansa jolla on lukuoikeudet käyttäjän **Desktop**-hakemistoon pääsee lukemaan niitä!

Myös kirjautumisaika pitenee, jos työpöydän työtiedostot kopioidaan työaseman kiintolevylle - ja taas takaisin palvelimelle, kun käyttäjä kirjautuu pois toimialueelta.

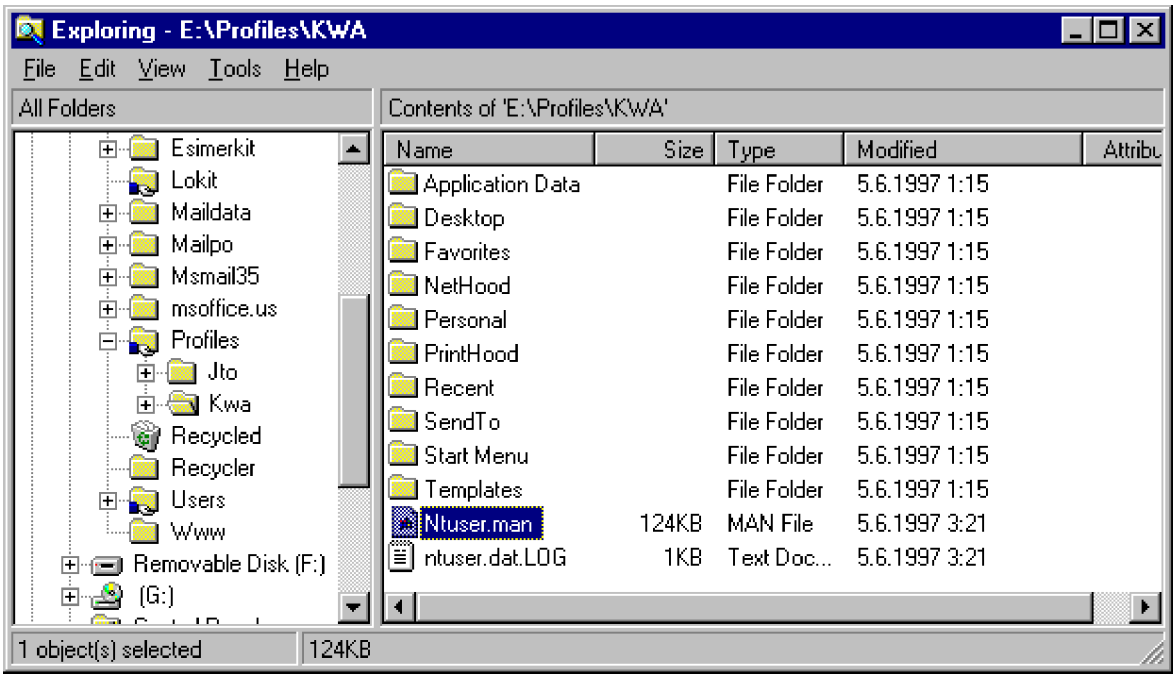
Kannattaa muistaa seuraavat seikat:

- Käyttäjät eivät saa tallentaa työtiedostojaan työpöydälle
- Profiilihakemistoon vain kyseisellä käyttäjällä on oikeuksia, minimissään **luku**-, enimmillään tietysti **täydet oikeudet** (muilla ei mitään)
- Profiili jää kiintolevylle, jos sitä ei erikseen poisteta rekisterin asetuksella (ks. myös Policy Editor).

Pakollinen profiili

Käy tämän jälkeen haluttaessa käyttäjälle **pakollinen profiili** (*Mandatory*) Resurssienhallinnalla muuttamalla kyseisessä hakemistossa tiedosto **NTUser.dat** nimelle **NTUser.man**. Tiedostotyyppi muuttuu samalla **MAN-tyyppiseksi**.

Tiedostotyypin muutto aiheuttaa sen, että käyttäjä ei voi muuttaa profiiliaan. Tällöin viimeksi profiilia käyttänyt käyttäjä ei muuta (vahingossakaan) profiilin asetuksia.



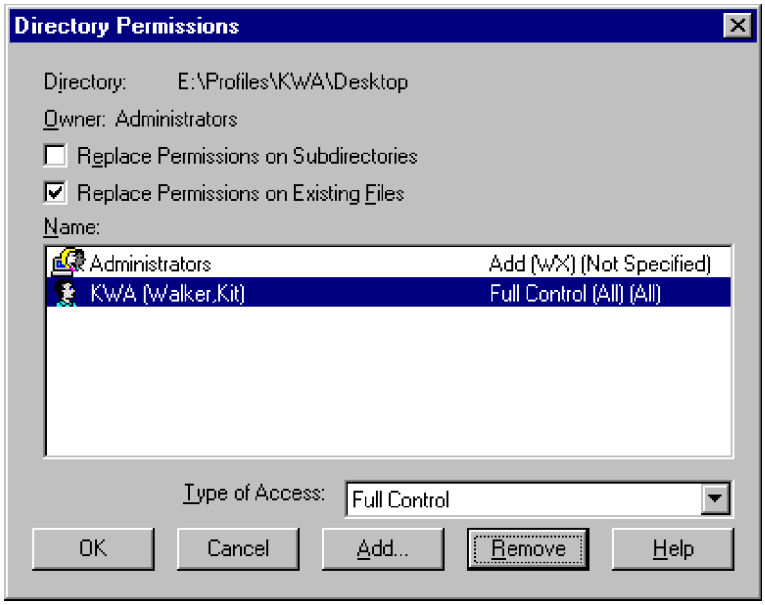
Lisäksi profiilihakemistoon vain kyseisellä käyttäjällä/käyttäjäryhmällä saa olla **lukuoikeudet** (muilla ei mitään). Poikkeuksena ehkä pääkäyttäjät, joilla voisi vain olla lisäysoikeus (**Add**) Desktop-hakemistoon (sen yläpuolisiin hakemistoihin luettelu (**List**)), jos halutaan keskitetysti ylläpitää palvelimella sijaitsevia profiileita.

Palvelimella sijaitsevien profiilien ylläpito

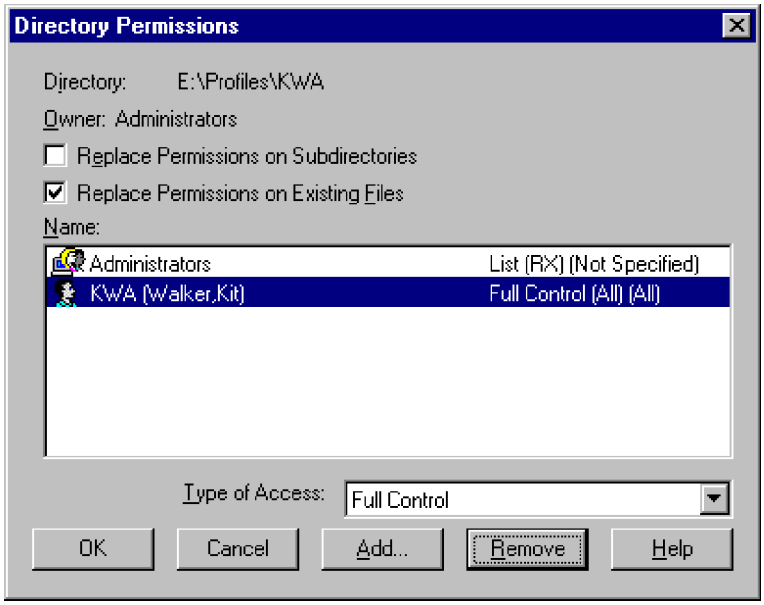
On myös mahdollista keskitetysti ylläpitää palvelimella sijaitsevia profiileita. Yksinkertaisinta lienee työpöydän kuvakkeiden ylläpito, mikä voidaan toteuttaa komentojonojen avulla. Tällä saadaan hieman tuntumaa siihen mitä *Zero Administration Windows* (**ZAW**) saattaisi merkitä.

Profiilihakemistoon vain kyseisellä käyttäjällä tai käyttäjäryhmällä saa olla **lukuoikeudet** (muilla ei mitään).

Jos halutaan ylläpitää työpöytien kuvakkeita, pääkäyttäjillä (Administrators) tulisi tällöin olla lisäysoikeus (**Add**) **Desktop**-hakemistoon. Tässä esimerkissä palvelimen **E:**-aseman jaetussa **Profiles**-hakemistossa on käyttäjäkohtaiset palvelimella sijaitsevat profiilit. Käyttäjän **KWA Desktop**-hakemistoon **Administrators**-ryhmällä on lisäysoikeus (**Add**).



Sen yläpuolisiin hakemistoihin (käyttäjän profiilihakemion päähakemisto) tarvitaan lisäksi luetteluoikeus (**List**), mutta tällä oikeudella ei voi lukea tiedostoja. Tässä esimerkissä palvelimen **E:**-aseman jaetussa **Profiles**-hakemistossa on **KWA**-hakemistossa käyttäjän **KWA** henkilökohtainen palvelimella sijaitseva profiili. Käyttäjän **KWA** profiilihakemistoon **Administrators**-ryhmällä on luetteluoikeus (**List**).



Myöskään lisäysoikeudella ei voi lukea tiedostoja, eli saavutetaan vähintään kohtuullinen tietoturvallisuus.

Jos halutaan kopioida **Profiles**-hakemistoon käyttäjän KWA työpöydälle kuvakkeita (dokumenttitiedostoja tai pikakuvakkeita), se voidaan toteuttaa esimerkiksi seuraavanlaisella komentojonolla:

```
COPY E:\DATA\COMMON\*.LNK E:\PROFILES\KWA\DESKTOP\*.*
COPY E:\DATA\KWA\*.* E:\PROFILES\KWA\DESKTOP\*.*
```

Tässä esimerkissä työpöytien kohteen on tallennettu kahteen hakemistoon: **Data**-hakemiston **Common**-hakemistossa on kaikille käyttäjille yhteiset kuvakkeet, ja käyttäjätunnuskohtaisessa hakemistossa on a.o. käyttäjälle tarpeelliset kuvakkeet. Kuvakkeet tulevat näkyviin, kun käyttäjä kirjautuu **seuraavan kerran** järjestelmään.

Komentojono saadaan hieman yleiskäyttöisemmäksi komentojonon parametrin **%1** avulla. Se saa arvokseen komentojonon toisen argumentin:

```
COPY E:\DATA\COMMON\*.LNK E:\PROFILES\%1\DESKTOP\*.*
COPY E:\DATA\%1\*.* E:\PROFILES\%1\DESKTOP\*.*
```

Jos e.m. komentojonon nimi on **UPDPROF.BAT**, niin komentorivin komennolla

```
UPDPROF KWA
```

päivitettäisiin käyttäjän **KWA** työpöydän kuvakkeet.

Kutsumalla komentojonoa **UPDPROF** toisesta komentojonosta (esim. (**BATCHUPD**) saadaan tilanne vielä helpommaksi. Voidaan päivittää useampi profiili seuraavasti:

```
CALL UPDPROF KWA
CALL UPDPROF KZY
CALL UPDPROF LLA
CALL UPDPROF LFI
jne...
```

Tämän jälkeen ei tarvitakaan kuin seuraavat temput:

1) Hieman puuhastelua **NET USER**-komennon avulla, jolla saadaan listaus käyttäjätunnuksista tiedostoon:

```
NET USER > LISTA.TXT
```

2) Otetaan tiedosto teksturin (**Notepad** käy) tai taulukkolaskentaohjelman (vaikkapa **Excel**) käsittelyyn ja tuotetaan rivit, jotka alkavat **CALL UPDPROF** ja sen jälkeen tulee käyttäjätunnukset. Tallennetaan tämä tiedosto nimellä **BATCHUPD.BAT**

3) Tarkista pääkäyttäjien oikeudet profiilihakemistoihin (ks. **CACLS**-komento)

3) Testataan **BATCHUPD.BAT**:in toiminta ja ajastetaan se. Apuna voidaan käyttää komentorivin komentoa **AT** (jolloin ajetaan **BATCHUPD.BAT** vaikkapa kahdesti päivässä) tai sopivaa viiveen aiheuttavaa apuohjelmaa, esimerkiksi Resource Kitin **SLEEP**, joka saa parametrikseen odotusajan sekunteina. Näissä esimerkeissä odotusaika on kaksi tuntia:

```
:START
CALL UPDPROF KWA
CALL UPDPROF KZY
CALL UPDPROF LLA
CALL UPDPROF LFI
jne...
SLEEP 7200
GOTO START
```

tai

```
CALL UPDPROF KWA
CALL UPDPROF KZY
CALL UPDPROF LLA
CALL UPDPROF LFI
jne...
SLEEP 7200
BATCHUPD
```

Default User

Käyttäjän ensimmäisellä kirjautumiskerralla **Default User** -kansion profiilia käytetään pohjana. Sen jälkeen käyttäjän ympäristö muodostuu seuraavasti:

- **All Users\StartMenu** ja käyttäjän oma **StartMenu** muodostaa **Käynnistys-valikon**
- **All Users\Desktop** ja käyttäjän oma **Desktop** muodostaa **Työpöydän**.

Jos kopioit **All Users**-hakemistoon sopivia pikakuvakkeita, ne tulevat käyttäjälle käyttöön hakemiston mukaiseen kohteeseen.

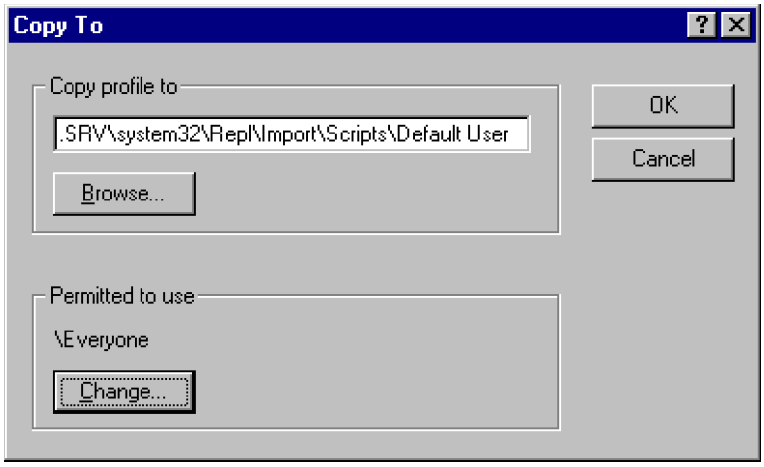
Tässä voi käyttää apuna vaikkapa kirjauskomentojonoja.

Default User palvelimella

Mikä on mielenkiintoista, on se, että **Default User** voidaan viedä myös palvelimelle. Jos luot palvelimen **NETLOGON**-jakoon **Default User**-kansio**n ja** käytät **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvaketta kopioidaksesi sopivan oletuskäyttäjän profiilin **Default User**-kansioon, sitä tullaan käyttämään uuden käyttäjän ensimmäisellä kirjautumiskerralla profiilin pohjana.

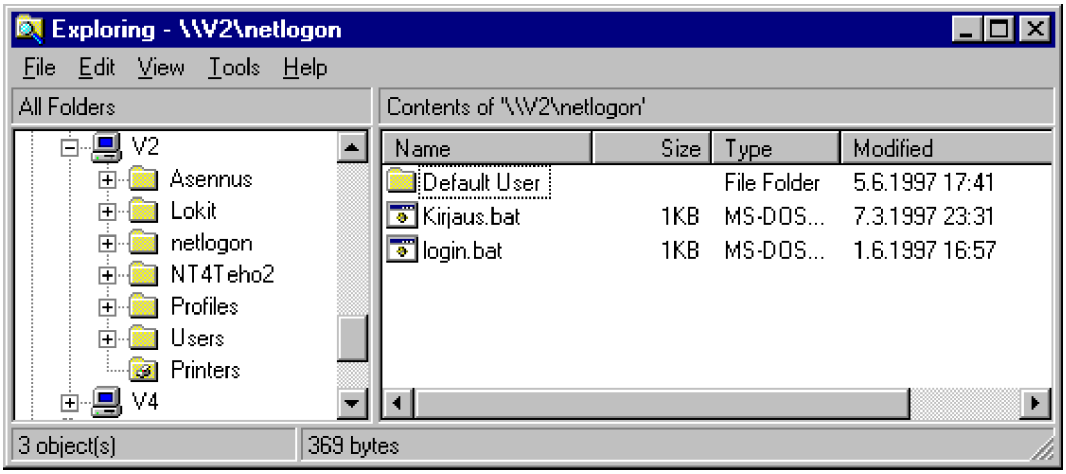
NETLOGON-jako on hakemisto **Winnt\System32\Repl\Import\Scripts**.

Kopioidessasi huomaa antaa oikeus käyttää profiilia esimerkiksi **Everyone**-ryhmälle.



Muista joko kopioida **Default User PDC**:n lisäksi kaikkiin **BDC**-palvelimiin tai käytä monistuspalvelua hyväksesi.

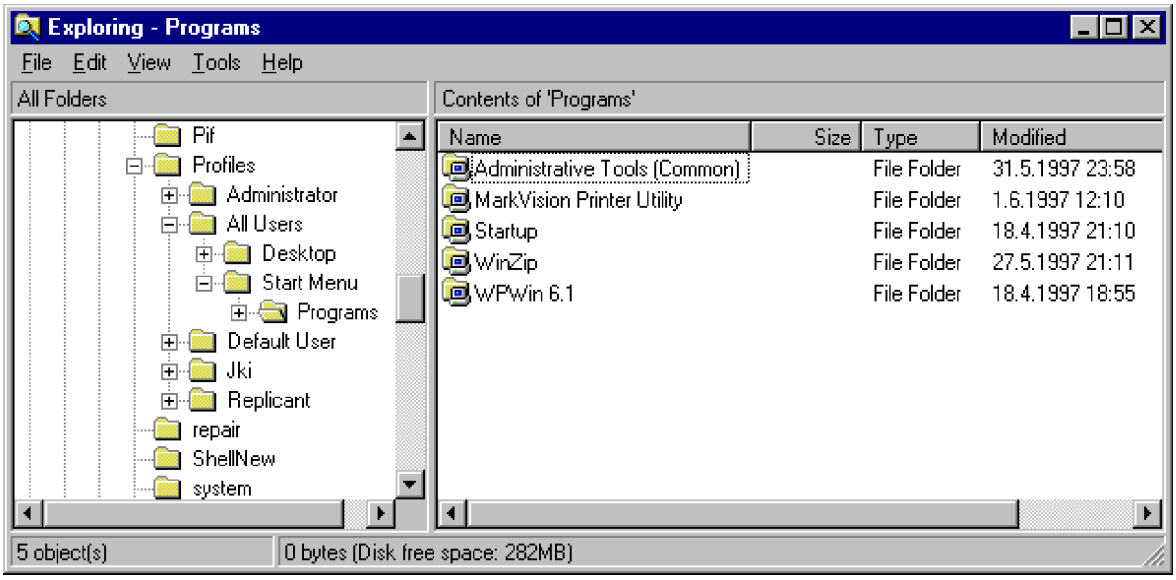
Kopioi tällöin **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeella **Default User** myös hakemistoon **Winnt\System32\Repl\Export**.



All Users

Kuten aiemmin mainittiin, **All Users\StartMenu** (ja käyttäjän oma **Start-Menu** muodostavat) **Käynnistys-valikon** ja **All Users\Desktop** (ja käyttäjän oma **Desktop**) muodostavat **Työpöydän**.

Jos kopioit **All Users**-hakemistoon sopivia pikakuvakkeita, ne tulevat käyttäjälle käyttöön hakemiston mukaiseen kohteeseen.



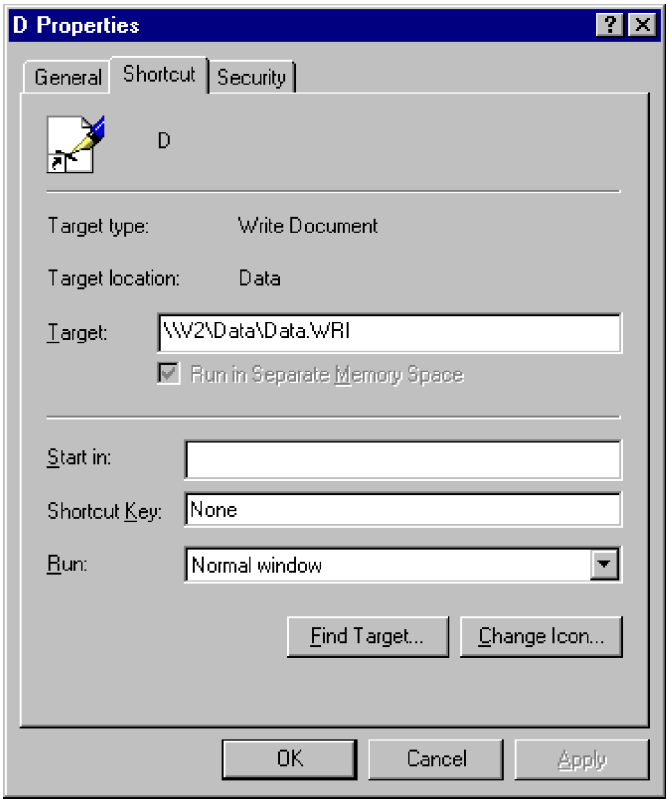
%USERPROFILE%-ympäristömuuttuja

Voit käyttää esimerkiksi kirjauskomentojonoissa hyväksesi ympäristömuuttujaa **%USERPROFILE%**. Se viittaa käyttäjän profiilihakemistoon.

Esimerkin komennot:

```
COPY \\V2\DATA\D.LNK %USERPROFILE%\DESKTOP
COPY \\V2\DATA\F.LNK %USERPROFILE%\DESKTOP
COPY \\V2\DATA\S.LNK %USERPROFILE%\DESKTOP
```

Kopioivat pikakuvakkeita käyttäjän työpöydälle.



Pikakuvakkeen on useimmiten syytä viitata UNC-nimellä johonkin verkon resurssiin. Esimerkin **D.LNK** viittaa **V2**-palvelimen jakaman **Data**-hakemiston **Data.wri**-tiedostoon.

Käynnistysvalikkoon tulee viitata esimerkiksi seuraavasti:

COPY \\V2\DATA\D.LNK %USERPROFILE%\"START MENU"

Lainausmerkit ovat siksi pakollisia, että hakemiston nimessä on välilyönti.

Esimerkiksi kokonainen uusi alivalikko **Programs**-hakemiston alle luotaisiin kahdella komennolla. Ensin luodaan hakemisto:

MD %USERPROFILE%\"START MENU"\Programs\Budjetti

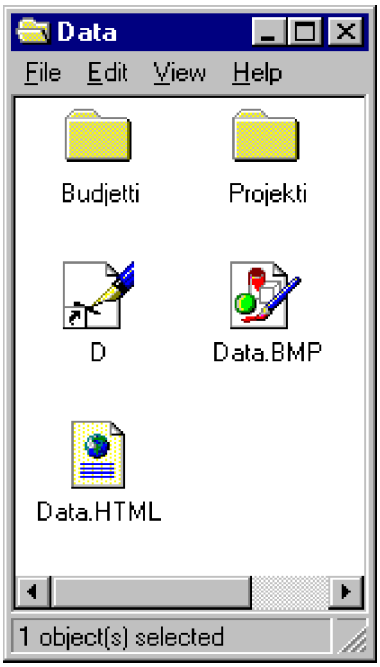
Ja sitten kopioidaan halutut pikakuvakkeet (komento jatkuu kahdella rivillä, jätä pois **--** -merkit):

COPY \\V2\DATA\Budjetti*.* %USERPROFILE%\"START --
MENU"\Programs\Budjetti

Seuraavaksi esimerkki, jossa tutkitaan käyttäjän **ryhmäjäsenyyttä**. Jos käyttäjä on **Administrators**-ryhmän jäsen, hänelle luodaan **System Tools**-alihakemisto. Käytetään hyväksi aiemmin esitettyä **IFMEMBER**-apuohjelmaa (komento jatkuu kahdella rivillä, jätä pois **--** -merkit):

```
ifmember Administrators
if not errorlevel 1 exit
MD %USERPROFILE%\"START MENU"\Programs\"System Tools"
COPY \\V2\DATA\PCTuki\*.* %USERPROFILE%\"START --
MENU"\Programs\"System Tools"
```

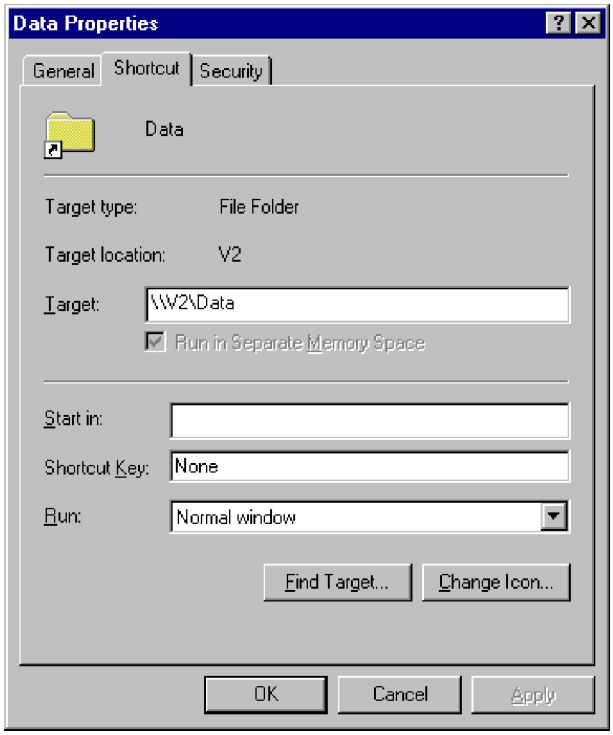
Muistathan, että pikakuvake voi olla viittaus **hakemistoon**. Tässä esimerkissä **Data.lnk** viittaa suoraan palvelimen **V2** jakamaan **Data**-hakemistoon.



Kopioidaan pikakuvake **Programs**-hakemiston:

```
COPY \\V2\DATA\Data.lnk %USERPROFILE%\"START MENU"\Programs
```

Pikakuvakkeen asetukset:



%SYSTEMROOT%-ympäristömuuttuja

Seuraavaksi luodaan kaikille käyttäjille yhteisiä pikakuvakkeita käyttämällä hyväksi **All Users**-hakemistoa ja **%SystemRoot%**-ympäristömuuttujaa.

Ongelma on se, että ei tiedetä missä hakemistossa **All Users**-hakemisto sijaitsee. Koska **All Users** sijaitsee järjestelmähakemiston alihakemistossa, siihen voidaan viitata järjestelmähakemiston **%SystemRoot%**-ympäristömuuttujalla.

Kopioidaan seuraavalla komennolla käyttäjille yhteisiä pikakuvakkeita työpöydälle (komento jatkuu kahdella rivillä, jätä pois **--** -merkit):

COPY \\V2\DATA\Desktop*.* %SYSTEMROOT%\PROFILES\ ALL --USERS \DESKTOP*.*

Työaseman FAT-levyllä tällä komennolla ei tule ongelmia, mutta NTFS-levyllä peruskäyttäjillä ei ole oikeuksia **All Users**-hakemistoon.

%COMPUTERNAME%-ympäristömuuttuja

Seuraavaksi kopioidaan käyttäjille yhteisiä pikakuvakkeita työpöydälle, jos työaseman nimi on **WS6** (komento jatkuu kahdella rivillä, jätä pois **--** -merkit):

if %COMPUTERNAME%x==WS6x COPY \\V2\DATA\Desktop*.* --
%SYSTEMROOT%\PROFILES\ ALL USERS \DESKTOP*.*

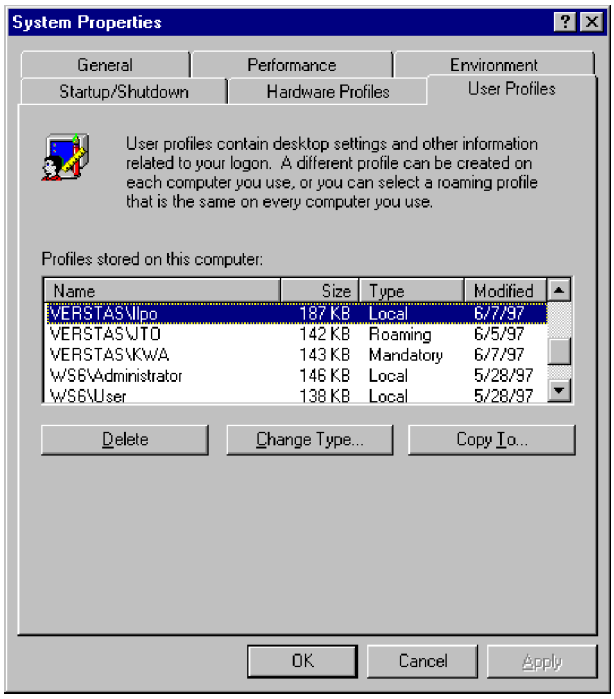
Työaseman FAT-levyllä tällä komennolla ei taaskaan tule ongelmia, mutta NTFS-levyllä peruskäyttäjillä ei ole oikeuksia **All Users**-hakemistoon.

Profiilin poistaminen

Profiili saataa kasvaa yllättävän suureksi, ja lisäksi profiilin työpöytä saattaa sisältää luottamuksellisia tietoja. NT-koneen levyllä olevan profiilin voit poistaa seuraavilla menetelmillä.

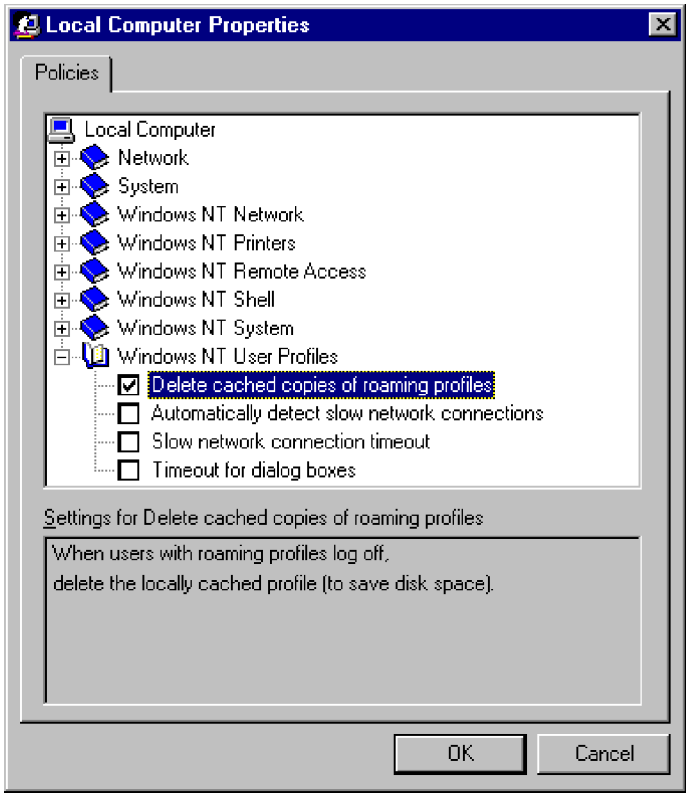
Ohjauspaneeli

Yksinkertaisin menetelmä on poistaa paikallisessa NT-koneessa olevat profiilit Ohjauspaneelin avulla. Tarvitset tähän pääkäyttäjän (Administrators) oikeudet kyseisessä NT-koneessa.



System Policy Editor

Toinen menetelmä on System Policy Editor, jolla voit määritellä palvelimella sijaitsevat profiilit poistettaviksi kun käyttäjä kirjautuu järjestelmästä.



Rekisteri

Edellinen asetus (palvelimella sijaitsevan profiilin poistaminen) on rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**DeleteRoamingCache**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei poisteta (oletus), 1 - poistetaan**

DELPROF

Neljäs menetelmä on Resource Kitin apuohjelma **DELPROF.EXE**. Tällä voi poistaa profiileita myös toisen NT-koneen levyltä.

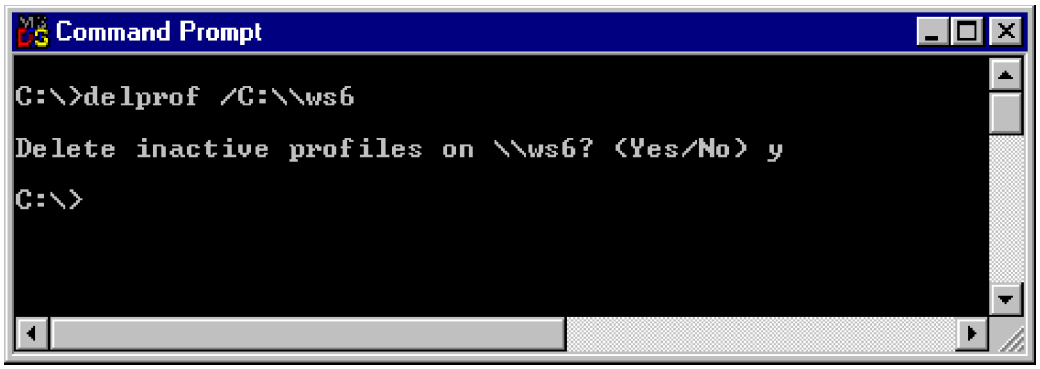
Syntaksi on:

DELPROF [/Q] [/I] [/P] [/C:\\<NT-kone>] [/D:<päiviä>]

Valitsimet ovat:

/Q Ei varmistusta
/I Ei pysähdytä virheisiin, vaan jatketaan poistamista
/P Kysytään varmistus ennen poistoa
/C Etäkoneen nimi
/D Käyttämättömän profiilin ikä.

Esimerkki: poistetaan vanhat ja ei-aktiivit profiilit NT-työasemasta **WS6**:



Pienenä varoituksena mainittakoon, että kyseiseen NT-koneeseen ei todennäköisesti jää muuta kuin a.o. hetkellä mahdollisesti kirjautuneen käyttäjän (aktiivi) profiili!

System Policy Editor

Järjestelmäkäytäntö (*System Policy*) tarkoittaa rekisterin määrityksiä, joilla voidaan rajoittaa entisestään Windows NT:n käyttöoikeuksia, asetusten muuttamista, verkkoon kirjautumista, salasanoja jne. Periaatteessa se toimii kuten Windows 95:n järjestelmäkäytäntökin, mutta ei ole tietenkään yhteensopiva.

Työpöydän käyttäjäprofiili-, kirjautumis- ja verkkokäyttöasetuksia säilytetään rekisteritietokannassa. **Käyttäjän järjestelmäkäytäntö** (*System policy for users*) korvaa rekisterin nykyisen käyttäjäalueen asetukset, ja **tietokoneiden järjestelmäkäytäntö** (*System policy for computers*) rekisterin paikallisen tietokoneen asetukset. Näin voidaan valvoa käyttäjien toimia (käyttäjäprofiileja) ja käyttäjien ja ryhmien käsittelyä.

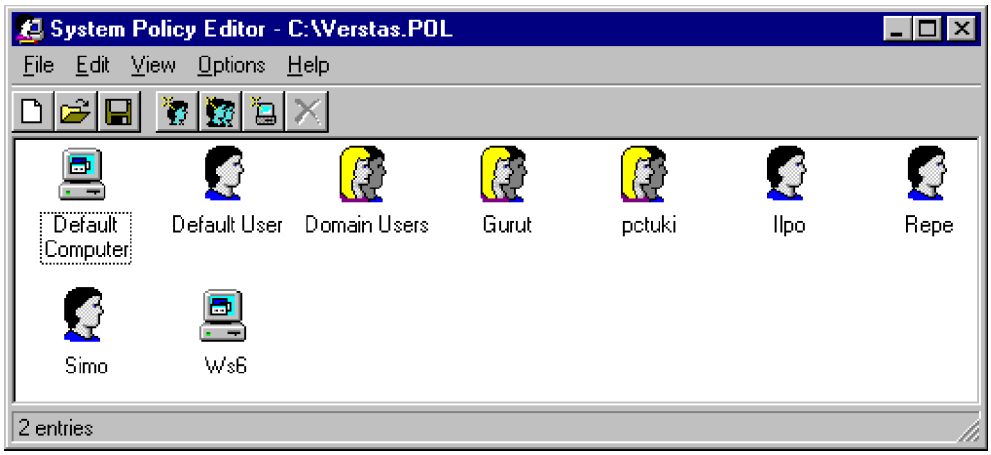
Järjestelmäkäytäntöjä käsitellään NT-palvelimen **System Policy Editorin** avulla. Voit asentaa **System Policy Editor**in myös Windows NT 4.0-työasemaan Windows NT 4.0 -palvelimen CD-ROM:ilta **Clients\Srvtools\Winnt**-kansiosta komennolla **SETUP**.

Järjestelmäkäytäntöjen etuja ovat:

- Asetusten suojaaminen - järjestelmäkäytäntöjä voidaan käyttää missä tahansa Windows NT 4.0-mikrossa, myös ilman lähiverkkoa
- Lähiverkkoa käytettäessä voidaan keskittää asetukset ja hallita asetuksia keskitetysti **NTConfig.POL-tiedoston** avulla
- Rekisterin asetusten muuttaminen on selkeämpää kuin käytettäessä rekisterieditoria
- Asetukset voidaan ottaa käyttöön paikallisella tasolla, jolloin jokaisella mikroa käyttävällä on samat asetukset
- Asetuksissa voidaan määritellä oikeudet Ohjauspaneeliin ja sen objektien asetusten muuttamiseen, työpöytään ja sen objekteihin sekä näiden objektien muokkaamiseen ja verkon asetuksiin
- Asetuksissa voidaan tukeutua lähiverkkoon, jolloin **käyttäjäprofiilien** ja käyttäjätunnusten avulla **käyttäjäkohtaiset** ase-

tukset seuraavat käyttäjää, kirjoitautuipa hän verkkoon miltä työasemalta tahansa

- Voidaan ottaa käyttöön lisäksi käyttäjäryhmäkohtaiset ja työasemakohtaiset asetukset.



Helpotat järjestelmäkäytäntöjen käyttöä seuraavasti:

- Järjestelmäkäytäntöjen käyttöönotto on harkittua ja testattua
- Tunnet itsekin järjestelmäkäytäntöjen idean ja toteutuksen
- Testaillessasi toimintoa ota varmistukset rekisteristä
- Ole varovainen! Testaa kaikki asetukset huolellisesti eri käyttäjätunnuksilla ja eri työasemissa!
- Määrittele etäpäivitys käyttöön paikallisiin järjestelmäkäytäntöihin. Jos käyttäjiä / työasemia on useita kymmeniä, palvelimen / verkon tulisi olla tehokas. Seuraa verkon ja palvelimien kuormitusta!
- Seuraa Windows NT -palvelimella lokien avulla **NTCONFIG.POL**-tiedostojen käyttöä!

Järjestelmäkäytäntöjen periaate

Järjestelmäkäytäntöjen periaate on syytä ymmärtää hyvin, jotta ne voi ottaa käyttöön eikä sattuisi kömmähdyksiä.

Järjestelmäkäytäntöjä voidaan luoda System Policy Editorin avulla seuraavasti:

- Luodaan oletusasetukset tietokoneelle ja toimialueen käyttäjäkäytäntö
- Luodaan mukautettuja asetuksia, joita sovelletaan yksittäisiin käyttäjiin, käyttäjäryhmiin tai yksittäisiin NT-koneisiin
- Määritetään noutotapa ja paikka, josta käytäntö noudetaan kaikille tai joillekin käyttäjille.

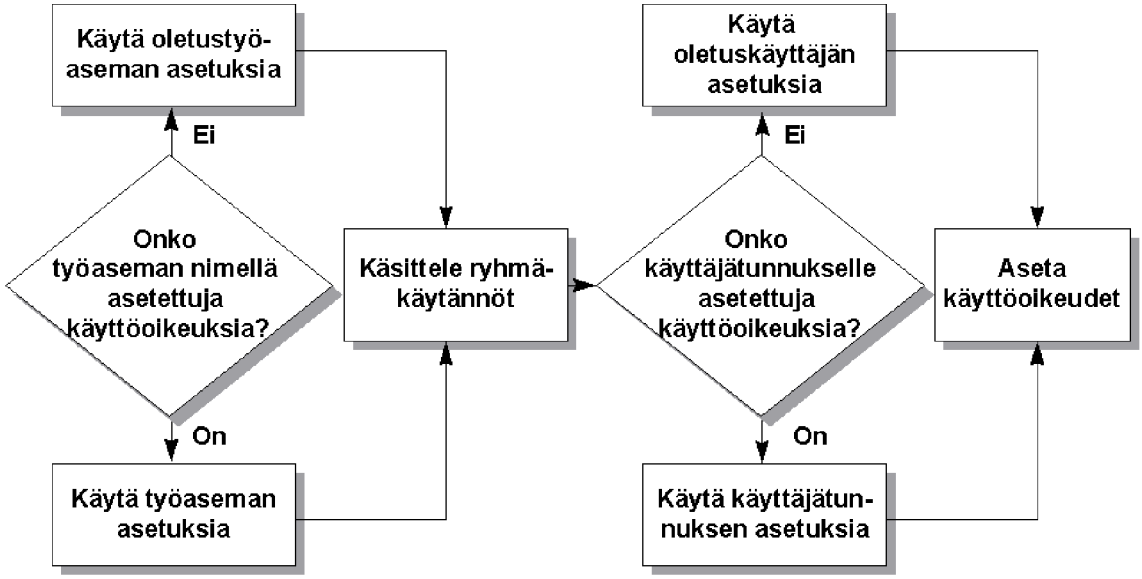
Seuraavat seikat vaikuttavat järjestelmäkäytäntöihin:

- **Oletuskäyttäjän** (Local User) ja **Oletustietokoneen** (Local Computer) asetukset. Nämä ovat itse asiassa paikallisen rekisterin asetuksia. **System Policy Editorissa** voidaan hallita käyttäjäasetuksia muuttamalla **Default User** -asetuksia ja kirjautumis- ja verkkoasetuksia muuttamalla **Default Computer** -asetuksia. Asetukset menevät rekisteriin **HKEY_CURRENT_USER**- ja **HKEY_LOCAL_MACHINE** -avaimiin
- Onko **työasemalle** luotu profiili. Tässäkin on varminta käyttää Windows NT:n verkkotukea ja sen oletuksia (**NTConfig.POL**)
- Kuuluuko käyttäjä johonkin **käyttäjäryhmään**, jolle on määritelty järjestelmäkäytäntöjä. Näiden voimaantulolla on oma järjestyksensä!

NTConfig.POL-tiedosto on **System Policy Editor**illa luotavissa oleva tiedosto, jonka Windows NT 4.0 osaa lukea verkon palvelimelta automaattisesti. Muuten voidaan luoda käyttäjäkohtainen POL-tiedosto, joka otetaan käyttöön UNC-polun takaa ns. **manuaalisella päivityksellä**, esimerkiksi **\\V1\Policy\JKI.POL**.

Oletuksena Windows NT 4.0 pyrkii lataamaan **NTConfig.POL**-tiedoston Windows NT -palvelimen **NETLOGON** -hakemistosta. Käyttäjällä tai käyttäjäryhmällä ja työasemalla voi olla omat asetuksensa. Ne voidaan tallentaa suoraan **NTConfig.POL**-tiedostoon. Jos tiedosto löytyy, sen sisältö kopioidaan paikallisen NT-koneen rekisteriin, ja sillä korvataan rekisterin senhetkiset käyttäjää ja paikallista NT-konetta koskevat osat.

Tällöin käsittelyjärjestys on seuraava:



Kun käyttäjä kirjautuu toimialueelle, palvelimen **NTConfig.pol** -tiedoston sisältö liitetään kirjautuvalle käyttäjälle löytyvän käyttäjäprofiilin **NTuser.dat**-tiedostoon. **NTuser.dat**-tiedoston **NTCofig.pol** -tiedoston tiedoista poikkeavat asetukset korvataan, ja järjestelmän asetukset valvovat siis koko toimialueen käyttäjäprofiiliasetuksia.

Ne **Default Computer** -asetukset, jotka eivät sisälly käyttäjäprofiiliin, lisätään rekisterin paikallista NT-konetta koskevaan osaan.

Kun yhteen käyttäjään sovelletaan useita eri käyttäjäprofiileja, erityistarkoitukseen suunniteltu käyttäjäprofiili ohittaa **käyttäjän ryhmän** käyttäjäprofiilin. Samoin jos käyttäjälle ei ole määritetty erityistä käyttäjäprofiilia, **käyttäjän ryhmän profiilia käytetään** (jos se on määritetty) ennen oletuskäyttäjäprofiilia (Default User).

Jos tietylle NT-koneelle ei ole määritetty profiilia, käytetään oletusprofiilia (Default Computer).

Jos käyttäjään sovelletaan useita eri ryhmäprofiileja, niiden järjestys määritetään **Group Priority** -ikkunassa.

Käyttäjien, ryhmien ja tietokoneiden asetusten muuttaminen

Jos jotkut käyttäjät, ryhmät tai NT-koneet vaativat erilaisia, oletusarvoista poikkeavia asetuksia, oletusasetuksia voidaan käyttäjiä, ryhmiä ja tietokoneita lisäämällä muuttaa siten, että halutut erityistarpeet otetaan huomioon.

Lisättävät käyttäjät, ryhmät tai NT-koneet saavat **NTConfig.pol** -tiedostoon omat merkintänsä, jotka sisältävät oletusarvoista poikkeavat asetukset:

- Kun järjestelmään kirjautuu käyttäjä tai ryhmän jäsen, jolle on **NTConfig.pol** -tiedostossa määritetty erityiset asetukset, järjestelmä hakee **NTConfig.pol** -tiedoston lisäksi myös käyttäjä- tai ryhmäkohtaiset asetukset.

- Jos System Policy Editoriin on lisätty NT-kone ja sille on määritetty erityisasetukset, jokainen siltä NT-koneelta kirjautuva käyttäjä saa NT-koneen asetukset. NT-koneen asetuksia käytetään, kun käyttäjä kirjautuu sisään. Asetukset haetaan käyttäjän kirjautumistoimialueelta, ei NT-koneen toimialueelta. Tästä voi seurata ongelmia, jos käyttäjä kirjautuu joskus sisään eri toimialueilta, jotka eivät kaikki käytä samoja asetuksia.

Sanotaanpa, että esimerkiksi **Pertillä** on käyttäjätunnus **Sumatra**-toimialueella ja hän matkustaa **Nepali**-toimialueelle. Toimialuieden välillä on luottosuhde.

Kun hän kirjautuu **Nepali**-toimialueella, hänen kirjautumispyyntönsä käsittelee **Sumatra**-toimialueella oleva kirjautumispalvelin.

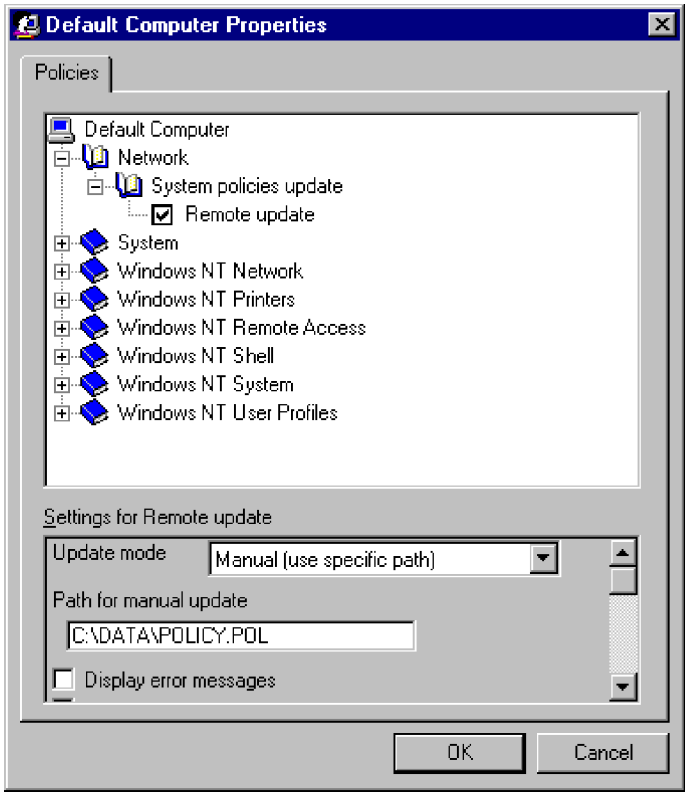
Jos sitten **Jurpo**, jolla on käyttäjätunnus **Nepali**-toimialueella, kirjautuu sisään **Pertin** kirjauduttua ulos eikä **Nepali**-toimialueella käytetä mitään järjestelmäasetuksia, **Sumatra**-toimialueen asetuksia ei korvata, vaan ne pysyvät voimassa!

Tästä seuraava ristiriitainen tilanne voidaan korjata ottamalla käyttöön järjestelmäkäytännöt kaikilla toimialueilla tai lataamalla erillinen käytäntö kaikille NT-koneille ns. **Manual-päivitystilan** avulla.

Manual-päivitystilan käytöllä varmistetaan, että järjestelmäkäytännöt kopioidaan aina tietyltä palvelimelta riippumatta siitä, kuka järjestelmään kirjautuu.

Kun järjestelmäkäytännöissä siirrytään automaattipäivityksestä manuaaliseen päivitykseen, määritetään joku muu polku kuin polku toimialueen PDC:n Netlogon-kansioon.

Jotta ominaisuutta voidaan käyttää, polku täytyy muuttaa tietokoneiden **System Policy Editoreissa**.



Toimintatilat ja mallitiedostot

Voit käyttää **System Policy Editoria** kahdessa eri tilassa:

- Työaseman **paikallisen rekisterin** tai **etähallitun työaseman rekisterin** käsittelyssä. Tällöin asetukset menevät samantien kyseisen työaseman rekisteriin! Tällöin käsitellään paikallisen rekisterin asetuksia. Kyseinen työasema on käynnistettävä uudelleen, jotta asetukset tulevat voimaan

- **Järjestelmäkäytäntötiedostojen** (.**POL**) muokkaamiseen. Näitä voit luoda aivan vapaasti, mutta suosittelen noudattamaan Windows NT:n oletuksia! Tämä on ns. *Policy File Mode*.

Järjestelmäkäytäntömallien (Templates) avulla voidaan määrittää järjestelmäkäytäntöjä verkon tietokoneille Windows NT Servereille, Windows NT -työasemille, Windows 95:lle tai niiden yhdistelmille (Windows 95 -tietokoneissa täytyy mahdollistaa käyttäjäprofiilit jokaisella Windows 95-konessa erikseen). Järjestelmäkäytännöt, jotka tulevat näkyviin, riippuvat käytetystä **mallitiedostosta**. Se määrittelee käytettävissä olevat asetukset, oletukset, painikkeet jne. Mallitiedosto on teksti (ASCII)-tiedosto.

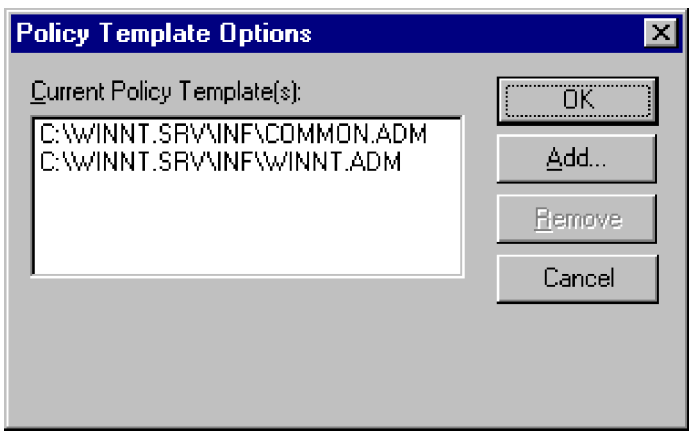
Kun **System Policy Editor** käynnistyy, se lukee kaksi oletusmallitiedostoa **%SystemRoot%\Inf**-hakemistosta:

- **Common.adm** - Windows NT 4.0:n ja Windows 95:n yhteisiä asetuksia, jotka luetaan **Commpn.adm**-tiedostosta: **Network**, **System**, **Desktop**, **Shell**, **Control Panel** ja **System**

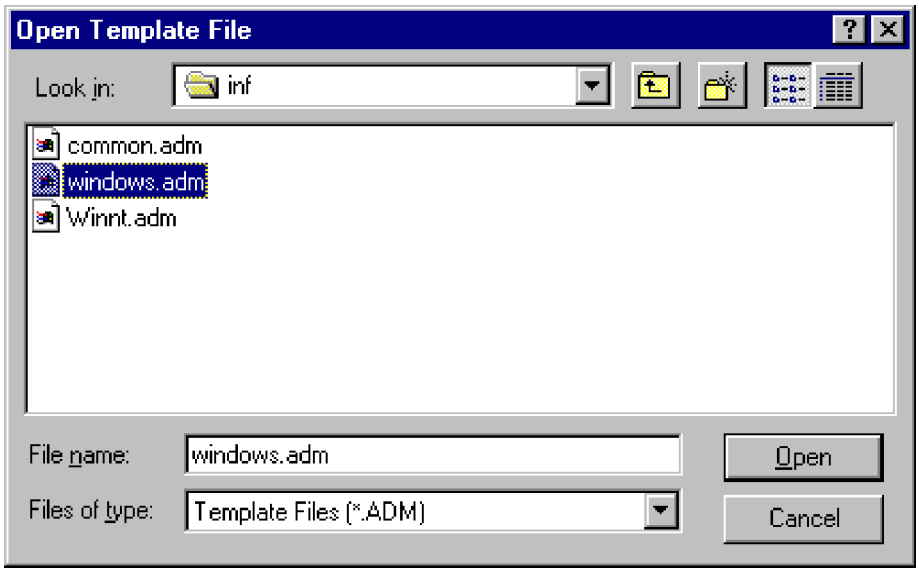
- **Winnt.adm** - Windows NT 4.0:n omat asetukset: **Windows NT Network**, **Windows NT System**, **Windows NT Printers**, **Windows NT Remote Access**, **Windows NT User Profiles**, **Windows NT Shell** ja **Windows NT System**.

Windows NT 4.0:n mukana tulee lisäksi mallitiedosto Windows 95:n asetuksille (**Windows.adm**), jossa ovat seuraavat: **Windows 95 Control Panel**, **Windows 95 Shell**, **Windows 95 System** ja **Windows 95 Network**. Tätä ei ladata oletuksena.

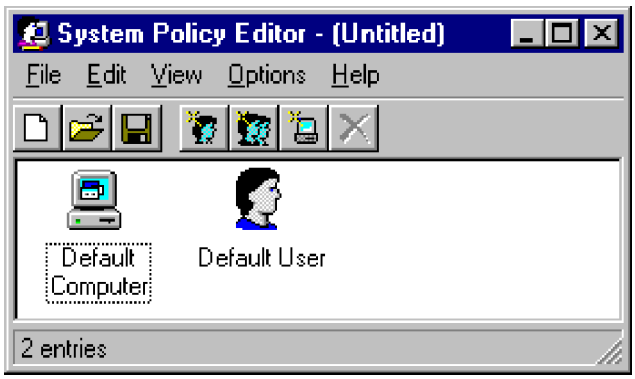
Mallien asetukset löytyvät valinnalla **Options** | **Policy Template**.



Valinnalla **Add** voit lisätä muita mallitiedostoja, ne löytyvät **Winnt\Inf**-hakemistosta:



Kun luodaan uusi järjestelmäkäytäntötiedosto, System Policy Editorissa näkyy kaksi kuvaketta, jotka edustavat rekisterin tietokone- ja käyttäjäosia.
Kun napautetaan joko **Default Computer** (oletustietokone) - tai **Default User** (oletuskäyttäjä) -kuvaketta, esille tulee siihen liittyvä rekisterin osa.



Jokaisessa pääluokassa, aliluokassa ja asetuksessa on vaihtoehtoja tietokoneiden ja käyttäjien käyttäytymisen muuttamiseksi. Joillekin asetuksille voidaan valita valintaruutu tai tekstilaatikon vaihtoehto; toisiin täytyy syöttää tiettyjä tietoja.

Asetuksissa voidaan tyypillisesti valita kolme mahdollisuutta:

- Asetus ei ole valittu

  ☐ Remove Run command from Start menu

- Asetus on valittu

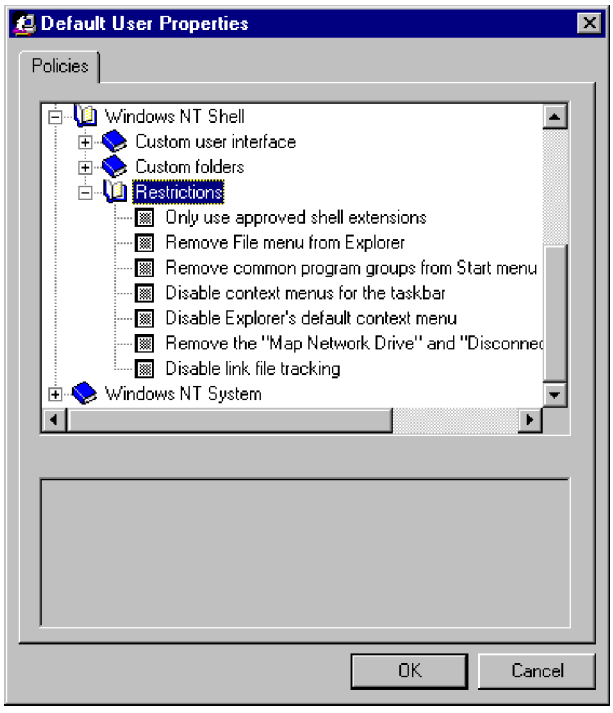
  ☑ Remove Run command from Start menu

- Asetukseen ei oteta kantaa (näitä asetuksia **ei** kopioida paikalliseen rekisteriin)

  ▩ Remove Run command from Start menu

System Policy Editorin valintaruuduissa on tavallisten valittu / ei valittu -vaihtoehtojen lisäksi kolmas vaihtoehto, joka on himmennetty. Tämän asetuksen tarkoitus on nimenomaan ilmaista, että rekisterin edellisiin asetuksiin verrattuna ei ole tapahtunut muutoksia. Kysymyksessä siis **ei** ole asetuksen poistaminen.

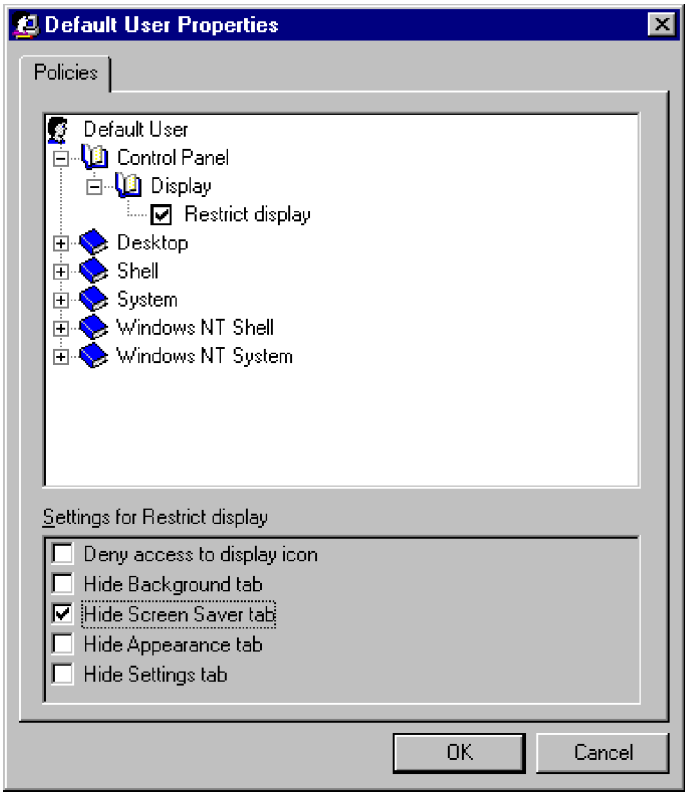
Joissakin System Policy Editorin asetuksissa käytetään termejä **disabled** (käyttö estetty), **removed** (poistettu) ja **hidden** (kätketty).



Termit ilmaisevat, miten kohde näkyy käyttäjälle:

- **disabled** - estetty komento näkyy valikossa himmennettynä
- **removed** - poistettu komento tai kohde ei näy valikossa
- **hidden** - käyttäjä ei näe kätkettyä komentoa.

Jos esimerkiksi valitaan **Hide Screen Saver Tab**, Ohjauspaneelin **Display**-asetusten **Screen Saver** -välilehti ei tule näkyviin.

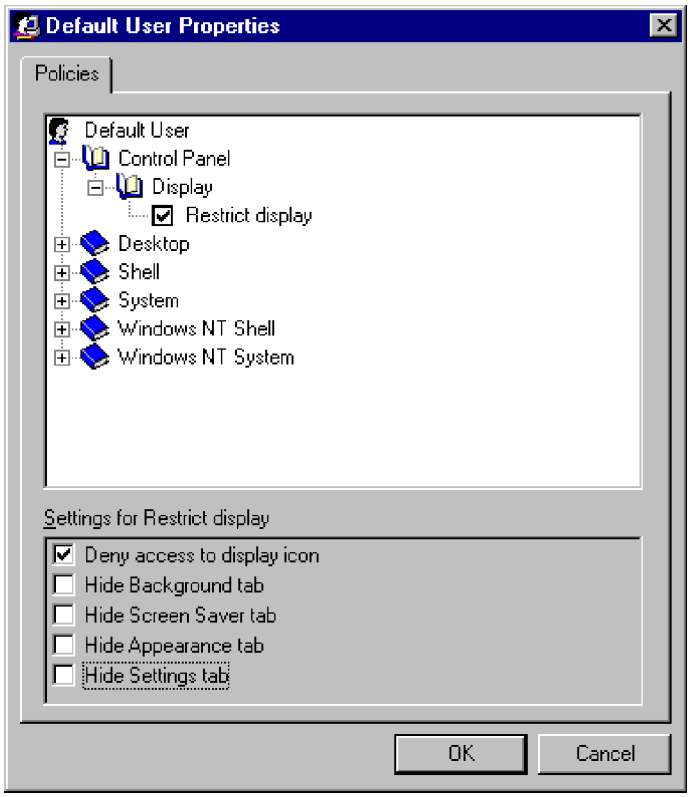


Käyttäjän asetukset

Default User -vaihtoehdolla voidaan hallita käyttäjäprofiilien asetuksia. Kukin **Default User Properties** -ikkunan vaihtoehto sisältää asetuksia, joiden avulla voidaan hallita, miten käyttäjä voi hallita käyttäjäympäristöään. Käyttäjälle muokattavissa olevia asetuksia käsitellään seuraavaksi.

Control Panel

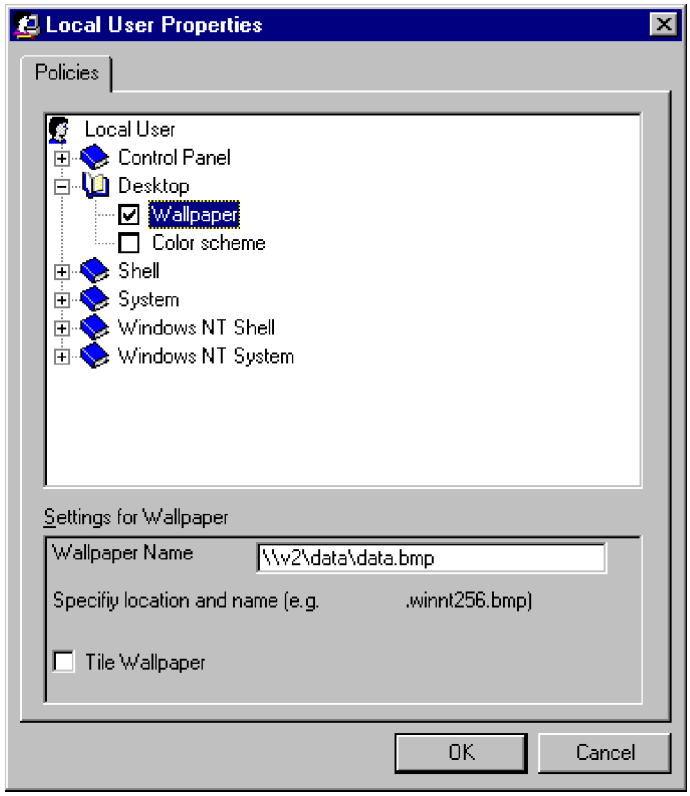
Display mahdollistaa näytön asetusten muuttamisen. Rajoita tällä vaihtoehdolla käyttäjän toimia Ohjauspaneelin Display-valinnoissa tai kiellä pääsy Display-ikkunaan (**Deny Access to display icon**). Voit piilottaa (**Hide**) yksitellen välilehdet: Background, Screen Saver, Appearance ja Settings



Tällöin ei kukaan käyttäjä (ei edes pääkäyttäjä) pääse muuttamaan näytön asetuksia.

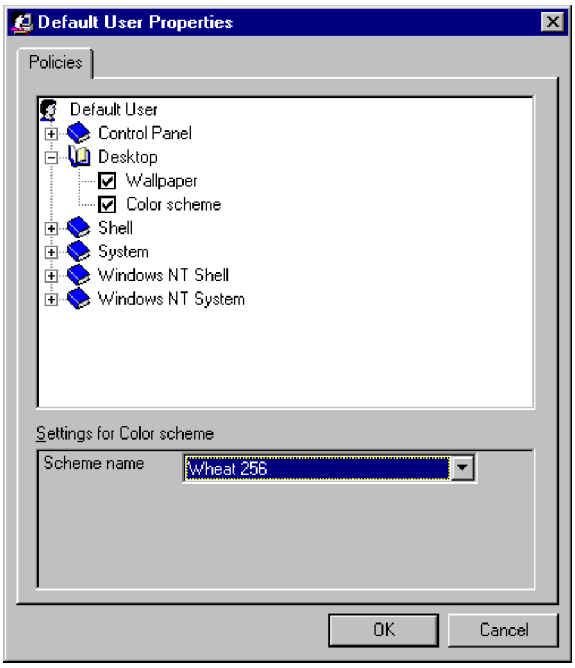
Desktop

Desktop määrittää työpöydän taustakuva ja värimallin asetukset:



- **Wallpaper** - taustakuvassa voit käyttää UNC-nimeä, esimerkissä viitataan polkuun **\\V2\DATA\DATA.BMP**. Tällöin voit keskittää (ja vaikka keskitetysti **vaihtaa**) näytön taustakuvat!

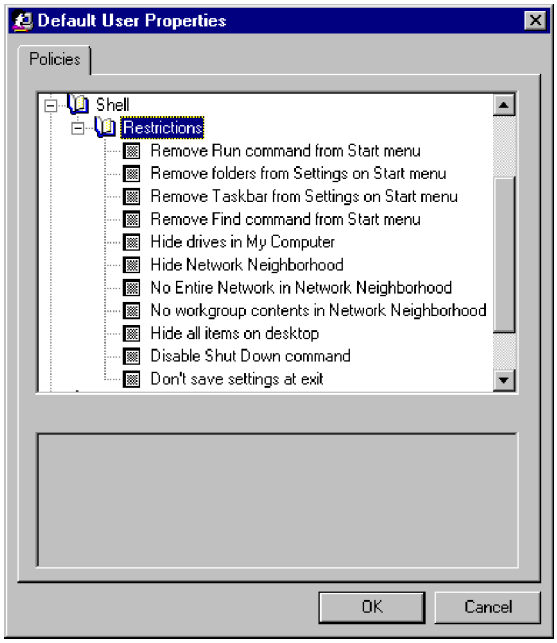
- **Color scheme** - värimalli, valitun värimallin on oltava asennettuna NT-koneessa.



Shell

Shell määrittää käyttöliittymän (Shell) asetukset. Voit mukauttaa työpöydän kansioita ja rajata työpöydällä näkyviä kohteita sekä Run-, Find- ja Shut Down -komentojen käyttöä.

Asetukset ovat seuraavat:



- **Remove Run command from Start menu** - poistaa **Suorita** (Run)-valinnan käynnistysvalikosta

- **Remove folders from Settings on Start menu** - poistaa kansiot asetuksista - tehtäväpalkki jää näkyviin

- **Remove Taskbar from Settings on Start menu** - poistaa myös tehtäväpalkin edellisistä!

- **Remove Find command from Start menu** - poistaa **Etsi** (Find)-valinnan käynnistysvalikosta

- **Hide drives in My Computer** - piilottaa levyasematunnukset **Oma Tietokone** (My Computer)-ikkunasta

- **Hide Network Neighborhood** - piilottaa verkkoympäristön

- **No Entire Network in Network Neighborhood** - ei näytä **Koko verkkoa** (Entire Network) verkkoympäristöstä, selailu ei tällöin onnistu

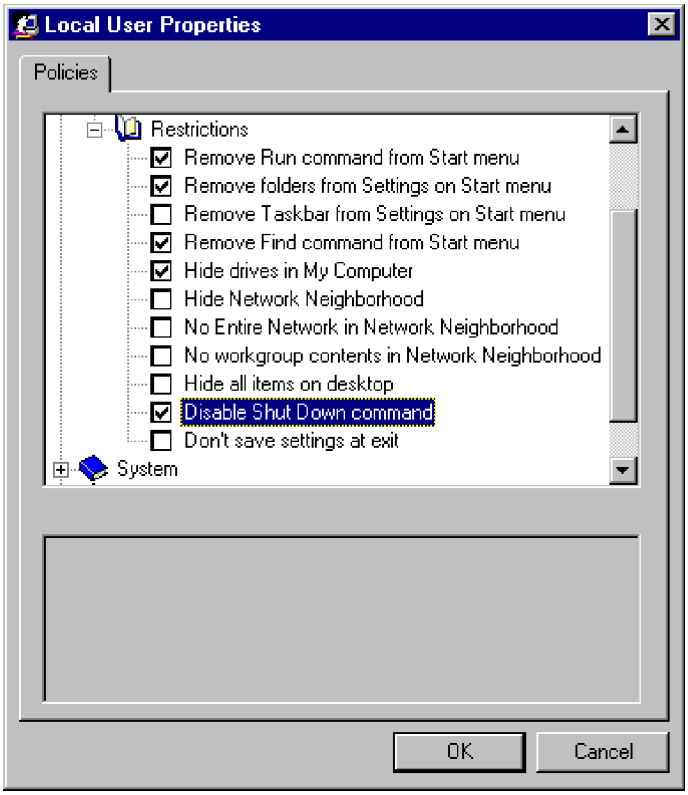
- **No workgroup contents in Network Neighborhood** - ei näytä työryhmän (tai toimialueen) sisältöä verkkoympäristöstä, työryhmän (tai toimialueen) selailu ei tällöin onnistu

- **Hide all items on desktop** - piilottaa kaikki työpöydän kuvakkeet

- **Disable Shut Down command** - poistaa **Sammuta** (Shutdown)-valinnan - tällöin kirjautuminen järjestelmästä tulee tehdä **Ctrl + Alt + Del**in tai **Alt + F4**:n avulla

- **Don t save settings at exit** - ei tallenna asetuksia poiskirjautumisen yhteydessä.

Esimerkki käyttöliittymän rajoituksista:



Valitut asetukset ovat:

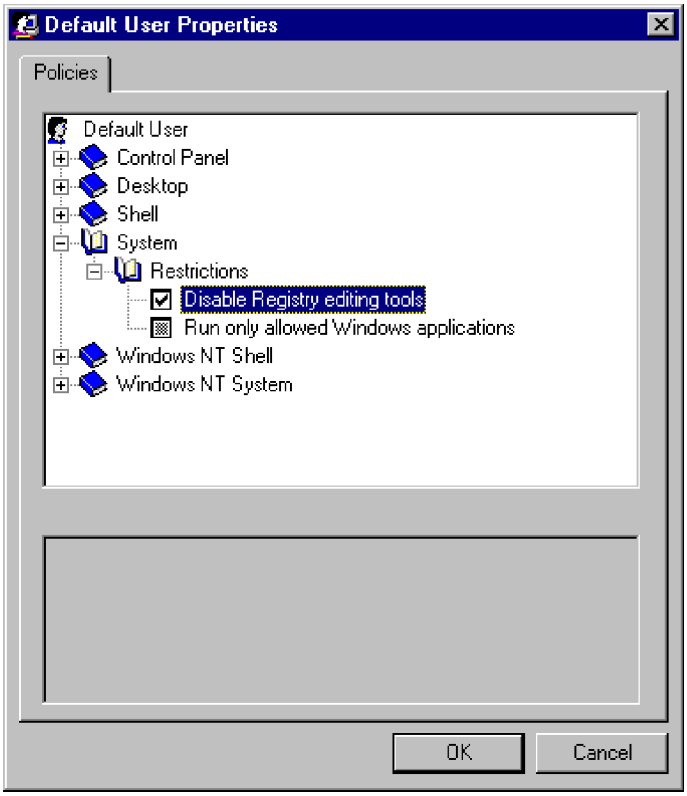
- Remove Run command from Start menu
- Remove folders from Settings on Start menu
- Remove Find command from Start menu
- Hide drives in My Computer
- Disable Shut Down command

Tällöin käynnistysvalikko (huomaa, että asetuksissa sallittiin tehtäväpalkin asetuksien muuttaminen) ja **Oma Tietokone** (My Computer) näyttää tältä:

System

Voit estää Windows NT Registry Editorin (**Regedt32.exe**) ja Windows 95 -tyyppisen rekisterieditorin (**Regedit.exe**) käytön, jolloin käyttäjät eivät voi muuttaa rekisteritiedostoja. Voit myös antaa luettelon sovelluksista, joita käyttäjät voivat käyttää. Jos sovellusta ei ole luettelossa, sitä ei voida käyttää.

Asetukset ovat seuraavat:



- **Disable Registry editing tools** - rekisterieditorien käyttö ei ole sallittu (kenellekään käyttäjälle!)

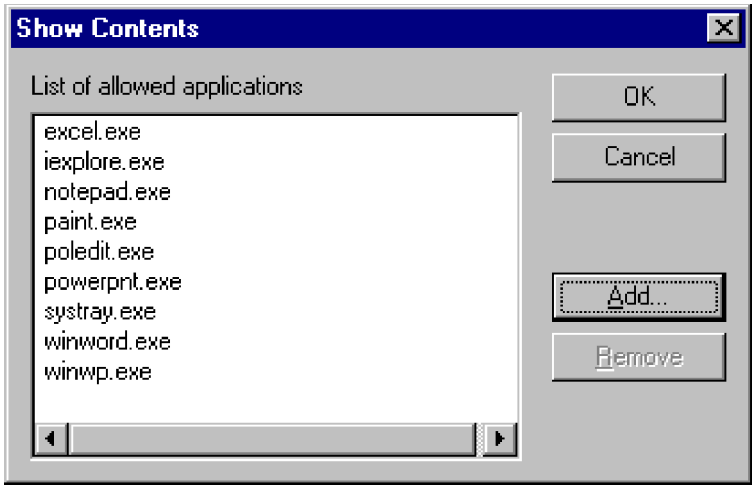
- **Run only allowed Windows applications** - lista sovelluksista, joita käyttäjät voivat käyttää. Voit lisätä sovelluksia painamalla **Show**. Muista lisätä luetteloon **POLEDIT.EXE**!

Esimerkki sovellusten rajoituksista:

Annetaan sallittujen sovellustiedostojen nimet:

- excel.exe
- iexplore.exe
- notepad.exe
- paint.exe
- powerpnt.exe
- poledit.exe
- systray.exe
- winword.exe
- winwp.exe

Muista aina lisätä luetteloon **POLEDIT.EXE**! Muussa tapauksessa saatat joutua muuttamaan asetukset esimerkiksi verkon kautta.



Jos saat kirjautumisvaiheessa ilmoituksen **This operation has been canceled due to restrictions in effect on this computer**, lisää sallittujen ohjelmatiedostojen listaan **SYSTRAY.EXE**. Se on ohjelma, joka lisää tehtäväpalkkiin **Käynnistä** (Start)-valikkoon osoittavan nuolen.

Jos sovellusta ei ole luettelossa, sitä ei voida käyttää:

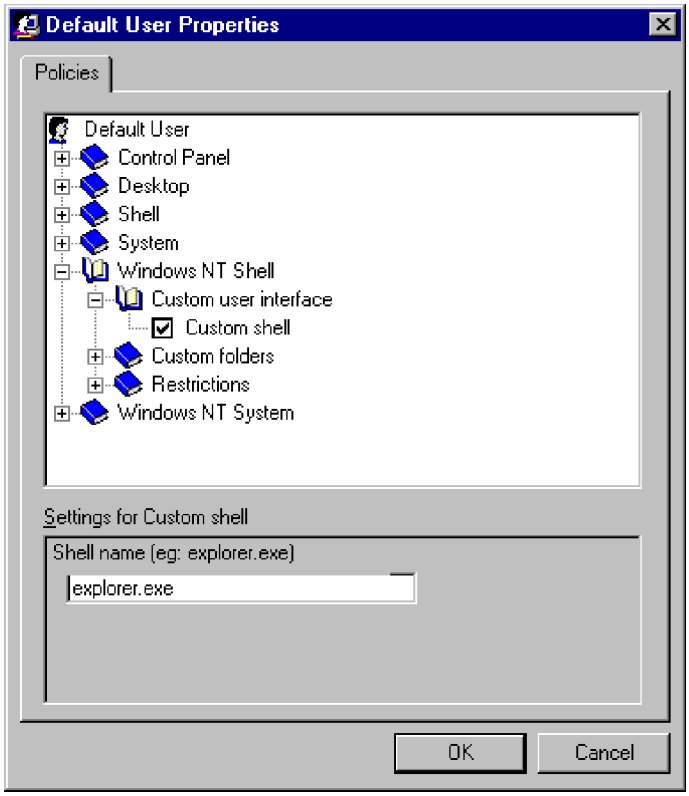
Kannattaa samalla suunnitella valikot ja niiden rakenteet tukemaan vain sallittujen sovellusten ajamista!

Windows NT Shell

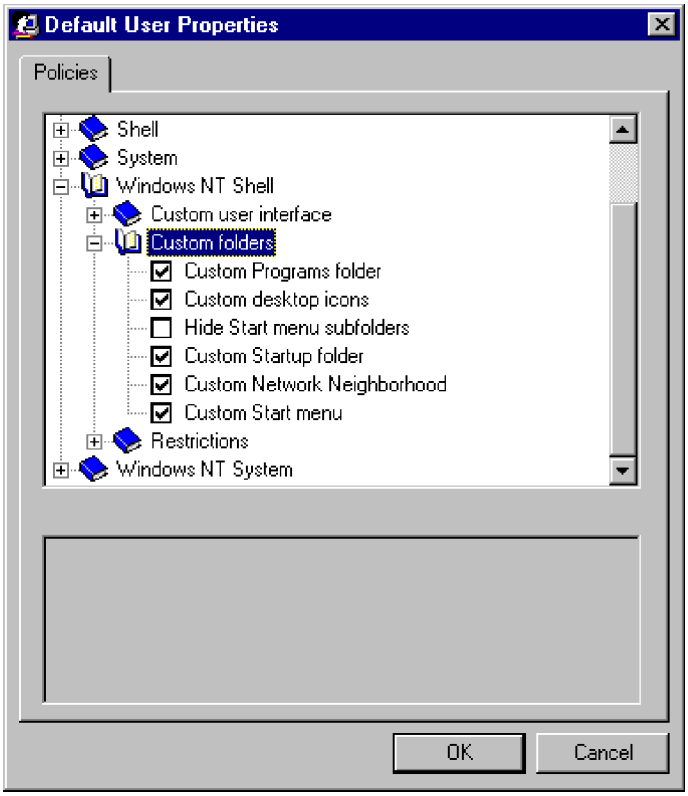
Lisää Windows NT:n käyttöliittymän (Shell) asetuksia. Työpöydän **kansioiden mukauttaminen** (Custom Folders) mahdollistaa käyttöliittymän asetusten muuttamisen viittaamalla muuhun kuin oletushakemistoon: voit luoda mukautettuja kansioita antamalla polkuja ohjelmakohteisiin, työpöydän kuvakkeisiin, käynnistyskohteisiin, Network Neighborhood -kohteisiin ja Käynnistä-valikon kohteisiin, joiden haluat tulevan jostain muualta kuin käyttäjäprofiilikansioista. Voit lisäksi määrittää sijainnin mukautetuille työpöydän kuvakkeille, Startup-kansioon haluttaville sovelluksille tai jopa korvata koko Käynnistä-valikon.

Custom user interface:

- **Custom Shell** - käyttöliittymän nimi, oletuksena **explorer.exe**. Tällä voidaan vaihtaa käyttöliittymäksi vaikkapa vain yksittäinen sovellus - kuten **Internet Explorer 3.0** tai **Internet Explorer 4.0**. Jos käytät tätä, anna koko polku sovelluksen ohjelmatiedostoon (ks. luvussa **11** Kioski-työasema)



Custom folders - kuvassa on valittu tyypilliset oletukset, joilla käyttäjän standardin mukainen profiili on käytettävissä:



- **Custom Programs folder** - käynnistysvalikon **Programs**-valikko viittaa oletuksena polkuun **%USERPROFILE%\Start Menu\Programs**. Muuttamalla tähän jotakin muuta **Programs**-valikkoa ei haeta käyttäjän profiilihakemistosta. Voit antaa **UNC**-polun, esimerkiksi **\\V2\PROFILES\PROGRAMS**

- **Custom desktop icons**- oletuksena työpöytä viittaa polkuun **%USERPROFILE%\Desktop**. Muuttamalla tähän jotakin muuta **työpöytää** ei haeta käyttäjän profiilihakemistosta. Voit antaa **UNC**-polun, esimerkiksi **\\V2\PROFILES\DESKTOP**

- **Hide Start menu subfolders** - piilotetaan käynnistysvalikon kansiot (Programs-valikko) - käytä jos valitset käyttöön **Custom Programs folder** tai **Custom Desktop icons**

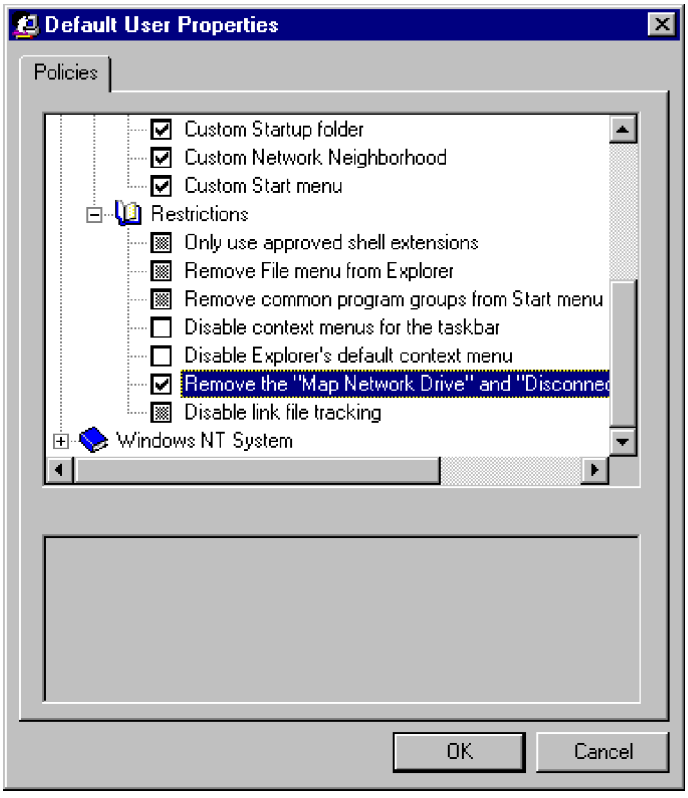
- **Custom Startup folder** - oletuksena automaattisesti käynnistettävien sovellusten jne kansio viittaa polkuun **%USERPROFILE%\Start Menu\Programs\Startup**. Tähän voi haluttaessa antaa jonkin muun, vaikkapa verkon palvelimen hakemiston!

Voit antaa **UNC**-polun, esimerkiksi **\\V2\PROFILES\STARTUP**

- **Custom Network Neighborhood** - oletuksena verkkoympäristö viittaa polkuun **%USERPROFILE%\NetHood**. Tähänkin voi **antaa** haluttaessa antaa jonkin muun polun, vaikkapa verkon palvelimen hakemiston UNC-polkuna, esimerkiksi **\\V2\PROFILES\NETHOOD**. Hakemistoon voi tallentaa vaikkapa **pikakuvakkeita verkon resursseista** (esimerkiksi **\\V1\DATA** tms), jolloin ne näkyvät **Network Neighborhood**-verkkoympäristössä. Erityisen tehokas tämä on, jos myös verkon selailu on estetty

- **Custom Start menu** - oletuksena käynnistyvalikko viittaa polkuun **%USERPROFILE%\Start Menu**. Tähänkin voi **antaa** haluttaessa antaa jonkin muun polun, vaikkapa verkon palvelimen hakemiston **UNC**-polkuna, esimerkiksi **\\V2\PROFILES\START**.

Restrictions:



- **Only use approved shell extension** - käyttöliittymän laajennusten (alivalikot, pikavalikot jne) salliminen

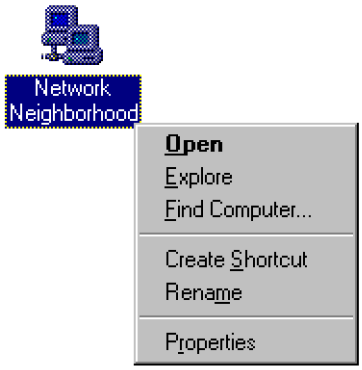
- **Remove File menu from Explorer** - Tiedosto (File)-valikko ei ole käytettävissä Resurssienhallinta-ikkunassa (Explore...)

- **Remove common programs groups from Start menu** - ei näytetä kaikkien käyttäjien yhteisiä ohjelmiryhmiä käynnistysvalikossa (All Users-hakemistosta)

- **Disable context menus from the taskbar** - poistetaan asetusten muuttaminen tehtäväpalkista (hiiren pikavalikko ei käytettävissä tehtäväpalkissa)

- **Disable Explorer s default context menu** - poistetaan Resurssienhallinta-valinta (Explore), jolloin hiiren pikavalikko ei käytettävissä

- **Remove the Map Network Drive and Disconnect Network Drive options** - poistetaan verkkoaseman kytkeminen tai katkaisu

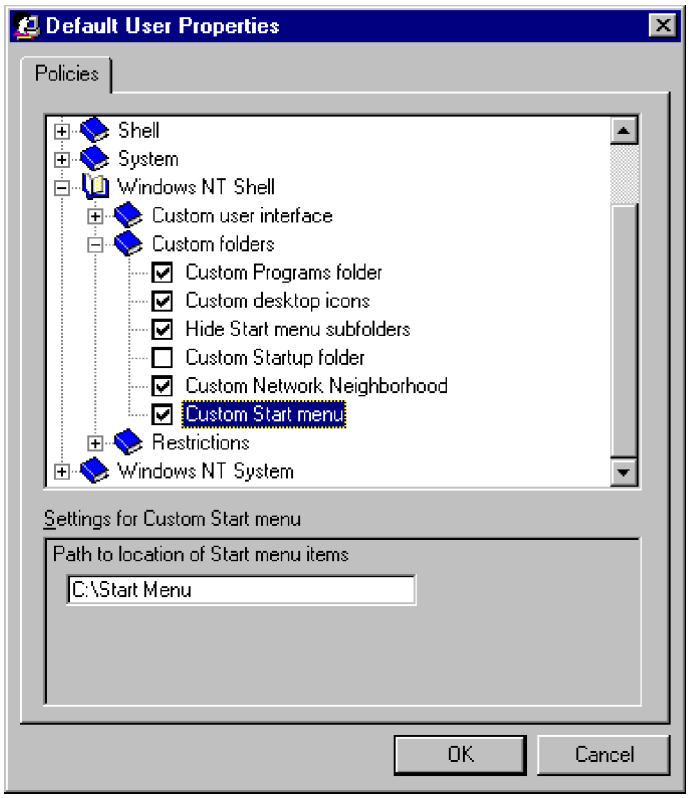


- **Disable link file tracking** - jos pikakuvakkeen kohde ei enaa ole olemassa, käynnistyy oletuksena selailu (**Browse**) - tällä selailun voi estää.

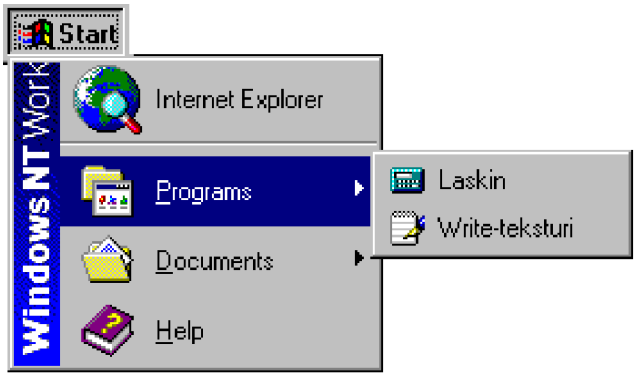
Esimerkki 1: rajoitetaan käynnistysvalikon valintoja.

Valitut asetukset ovat:

- **Custom Programs folder** - käynnistysvalikon **Programs**-valikko viittaa esimerkissä C:-aseman Progmans-hakemistoon,josta löytyvät **Calc.exe** ja **Write.exe**
- **Custom desktop icons**- saman tyyppinen menettely kuin edellä
- **Hide Start menu subfolders** - piilotetaan käynnistysvalikon muut valinnat
- **Custom Startup folder** - ei automaattisia käynnistyksiä
- **Custom Network Neighborhood** - saman tyyppinen menettely kuin edellä
- **Custom Start menu** - viittaus C:-aseman **Start Menu**-hakemistoon,josta löytyy **IEXPLORE.EXE**
- **Remove common programs groups from Start menu** - ei näytetä yleisiä ohjelmaryhmiä.



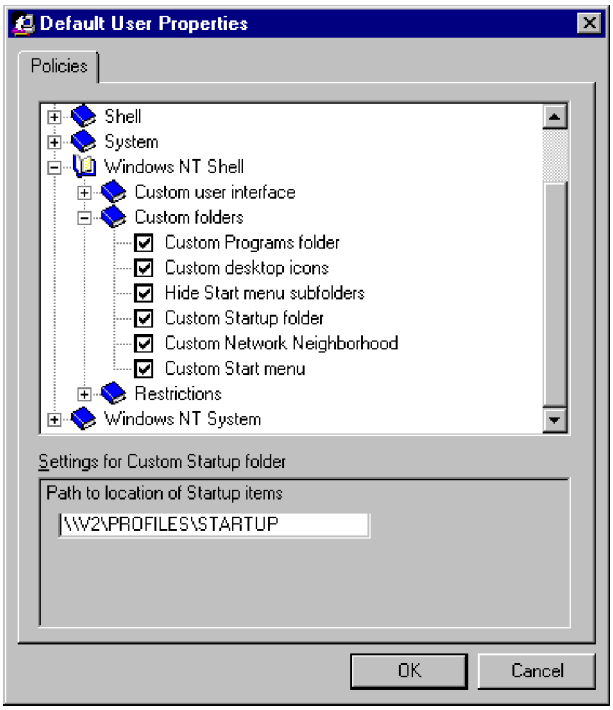
Käynnistysvalikko näyttää tältä:



Esimerkki 2: käyttäjän käynnistysvalikko haetaan palvelimelta.

Valitut asetukset ovat:

- Custom Programs folder - \\V2\PROFILES\PROGRAMS
- Custom desktop icons - \\V2\PROFILES\DESKTOP
- Hide Start menu subfolders - piilotetaan käynnistysvalikon kansiot
- Custom Startup folder - \\V2\PROFILES\STARTUP
- Custom Network Neighborhood - \\V2\PROFILES\NETHOOD
- Custom Start menu - \\V2\PROFILES\START
- Remove common programs groups from Start menu - ei näytetä yleisiä ohjelmaryhmiä.

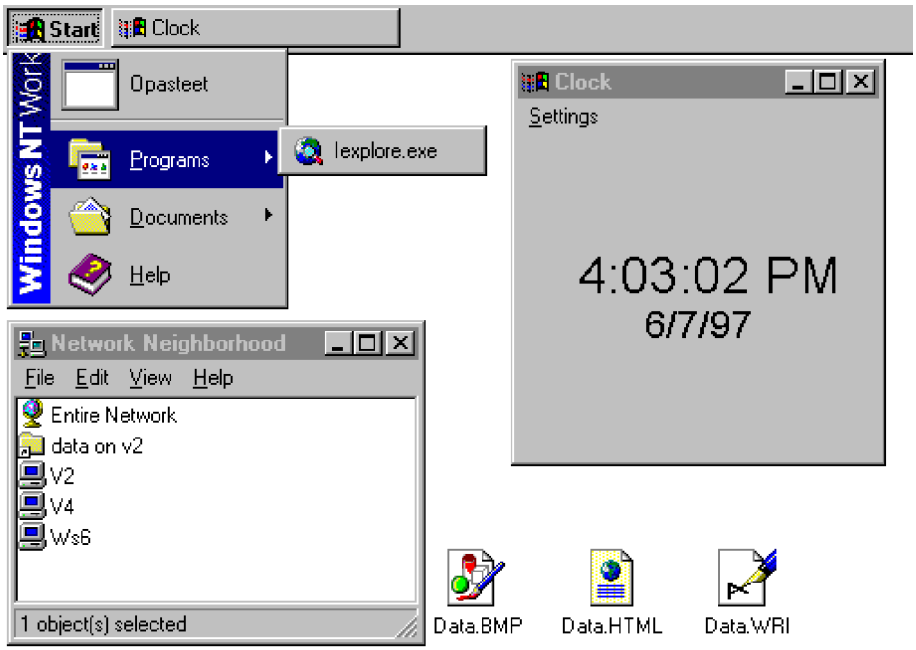


UNC-polut ja hakemistojen sisältö esimerkissä on seuraava:

UNC-polku	Sisältö
\\V2\PROFILES\PROGRAMS	Iexplore.exe
\\V2\PROFILES\DESKTOP	Data.bmp, Data.HTML, Data.WRI
\\V2\PROFILES\STARTUP	Clock.exe
\\V2\PROFILES\NETHOOD	Pikakuvake, UNC-polku on \\V2\Data
\\V2\PROFILES\START	Opasteet.txt

Korvaa esimerkin hakemistot ja kuvakkeet omaan ympäristöösi sopiviksi.

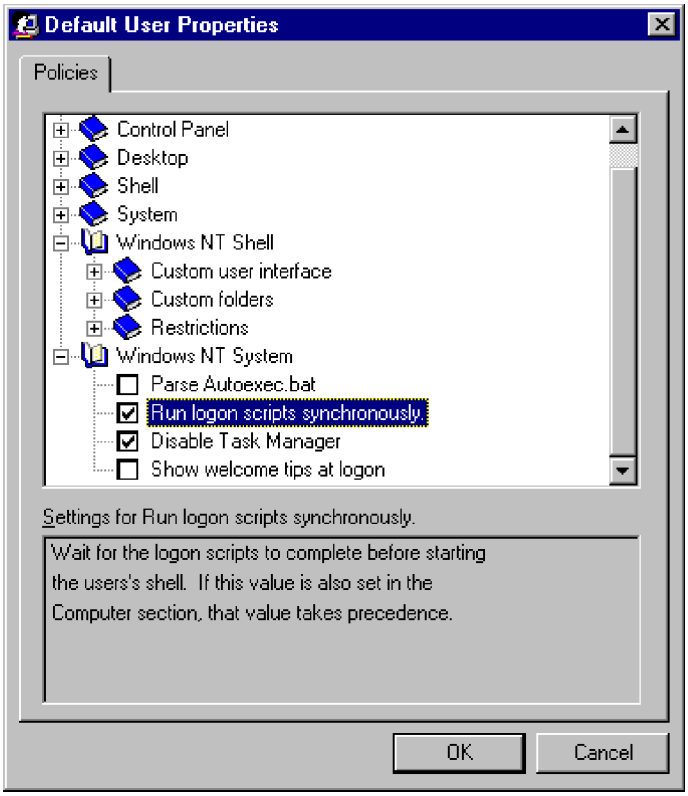
Käyttäjän kirjautuessa ympäristö näyttää tältä:



Windows NT System

Windows NT System mahdollistaa käynnistykseen liittyviä asetuksia:

- **Parse Autoexec.bat** - Windows NT lukee ympäristömuuttujat ja liittää ne käyttäjän ympäristömuuttujiin
- **Run Logon scripts synchronously** - tällä valinnalla ensin suoritetaan kirjauskomentojono, sitten vasta tulee käyttöliitymä käytettäväksi
- **Disable Task Manager** - poistaa tehtävänhallinnan käytöstä
- **Show welcome tips at logon** - ensimmäisen kirjautumisen yhteydessä tulee näkyviin päivän vinkki - tällä senkin voi estää.



Tietokoneen asetukset

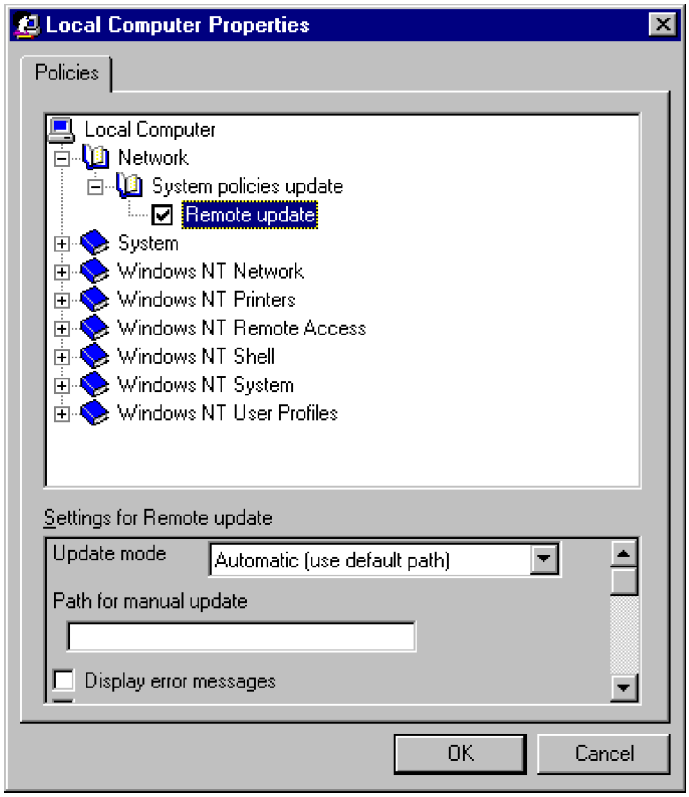
Tietokoneen käytännöissä (**Default Computer** tai **Local Computer**) määritellään kirjautumiskäytännöt ja verkkokäyttö.

Valinnat sisältävät asetuksia, joiden avulla käyttäjiltä voidaan estää käyttöjärjestelmän laitteisto- ja ympäristöasetusten muuttaminen.

Valittavissa on **Default Computer**, jos kohteena on järjestelmäkäytäntötiedosto, ja **Local Computer** jos kohtena on paikallisen NT-koneen rekisteri.

Network

Valinnat ovat seuraavat:



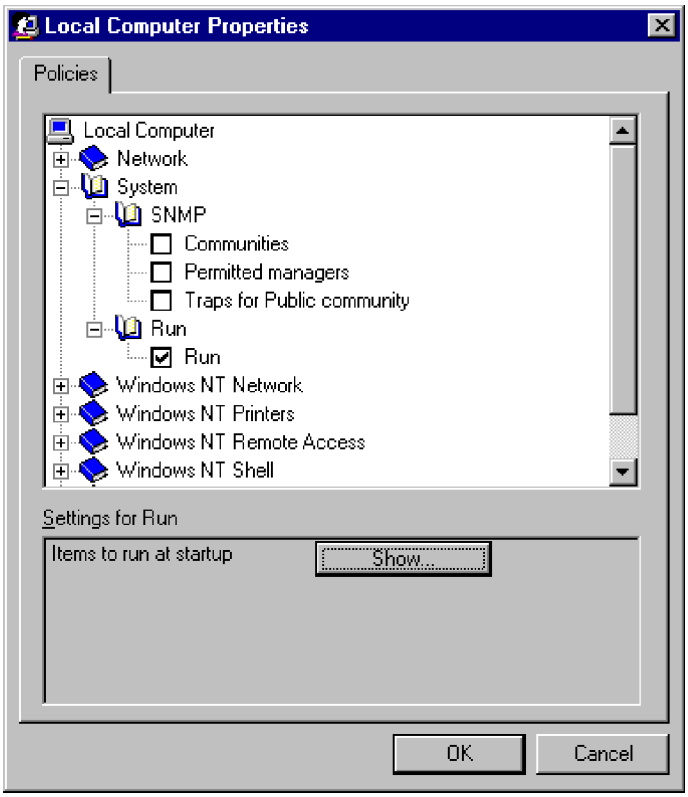
System policies update:

- **Display error messages** - virheilmoitukset aina, kun käytäntöä ei voida käyttää

- **Load Balancing** mahdollistaa järjestelmäkäytäntöjen hakemisen useilta eri ohjauskoneilta. Load Balancingin käyttöönotto estää laajojen verkkojen pullonkauloja, jos monet käyttäjät yrittävät samanaikaisesti käyttää samaa käytäntötiedostoa.

System

System antaa mahdollisuuden määritellä mm. **SNMP** (*Simple Network Management Protocol*):n asetuksia.

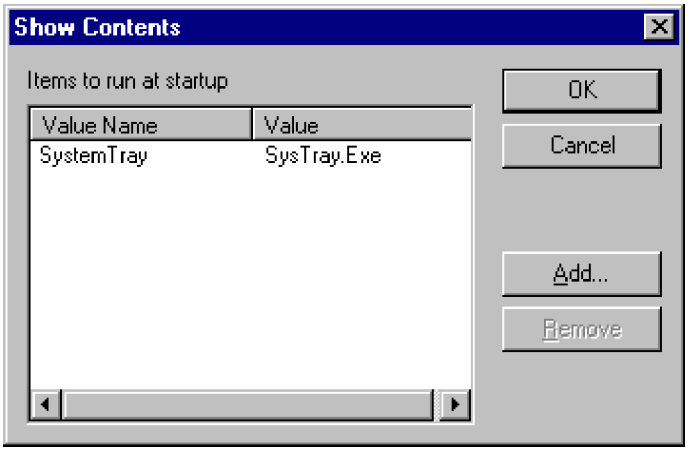


SNMP:

- Voit muuttaa oletusarvoista SNMP-konfiguraatiota lisäämällä yhteisö- ja valvonta-asetukset (communities, managers ja public community traps). Näiden oletusarvot määritetään, kun SNMP-palvelu konfiguroidaan isäntäkoneella. Järjestelmässä on kolme vaihtoehtoa SNMP:n oletusarvojen muuttamiseksi

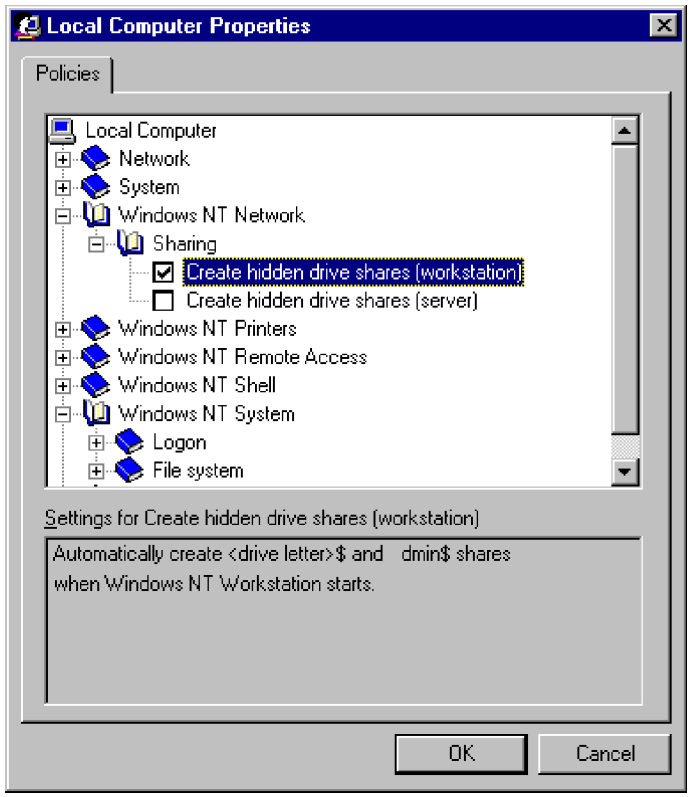
Run:

- **Run** - voit määrittää Run-kohtien sisällön, jolla määritetään, mitkä sovellukset ajetaan käynnistysvaiheessa. Oletus on **SYSTRAY.EXE**. Se on ohjelma, joka lisää tehtäväpalkkiin **Käynnistä** (Start)-valikkoon osoittavan nuolen.



Windows NT Network

Windows NT Network -asetuksilla määritetään piilotetut jaetut resurssit.

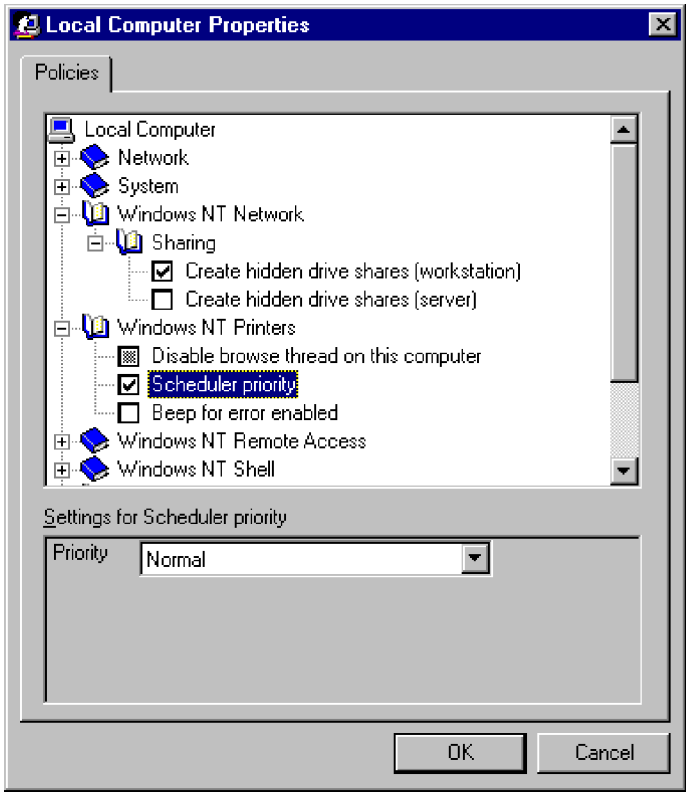


Sharing:

- **Create hidden drive shares (workstation)** - luodaanko työasemassa piilotetut jaetut resurssit
- **Create hidden drive shares (server)** - luodaanko palvelimessa piilotetut jaetut resurssit.

Windows NT Printers

Windows NT Printers -asetuksilla määritellään kirjoittimien lisäasetuksia.



Valinnat ovat:

- **Disable browse thread on this computer** - tulostuspalvelimilla voidaan estää tulostusjonon selailuprosessi, joka lähettää säännöllisin väliajoin toisille tulostuspalvelimille tietoa siitä, mitkä palvelimen kirjoittimet on jaettu. Selailu kuluttaa jonkin verran

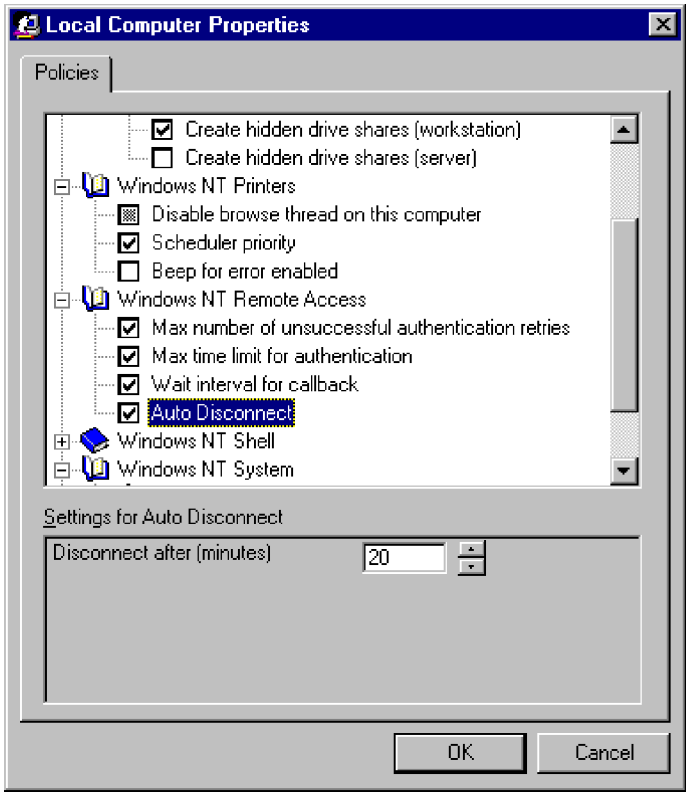
suorittimen ja verkon tehoa, eikä sitä välttämättä tarvita tulostamiseen

- **Scheduler priority** - voit muuttaa tulostustöiden prioriteettia porteissa

- **Beep on error enabled** - voit asettaa tulostusjonon seuraajan antamaan merkkiäänen 10 sekunnin välein, jos etätulostuksessa on tapahtunut virhe.

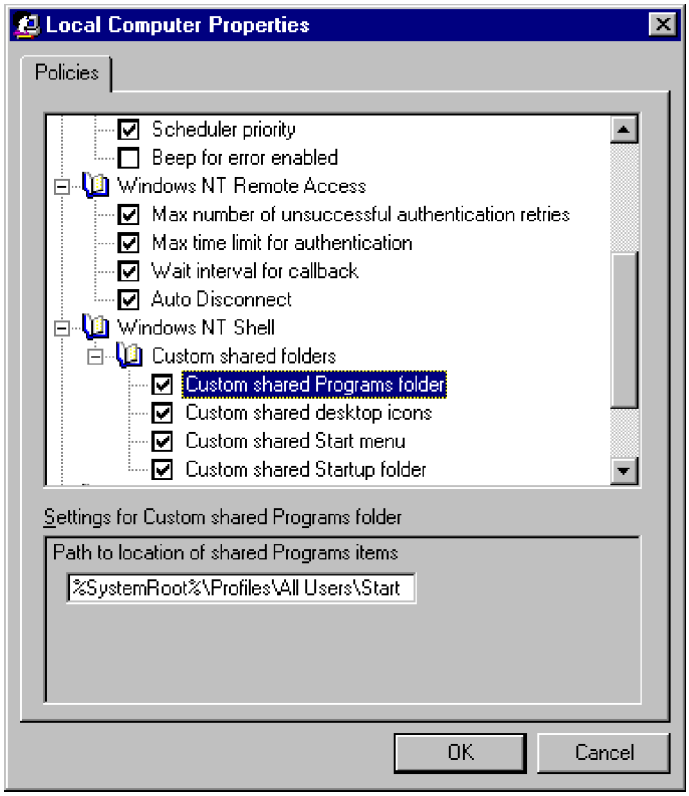
Windows NT Remote Access

Kun käytetään etäkäyttöpalvelinta, voidaan määrittää epäonnistuneiden kirjautumisyritysten maksimimäärä ja kirjautumisen maksimiaika. Voit myös määrittää ajanjakson takaisinsoittoyritysten välillä ja aikarajan automaattiselle aikakatkaisulle.



Windows NT Shell

Tämän avulla voidaan määritellä kaikkia käyttäjiä koskevia käyttöliittymän asetuksia.



Custom shared folders:

- **Custom shared Programs folder** - käynnistysvalikon **Programs**-valikko viittaa oletuksena polkuun **%SystemRoot%\Profiles\All Users\Start**. Muuttamalla tähän jotakin muuta **Programs**-valikkoa ei haeta **All Users**-profiilihakemistosta. Voit antaa **UNC**-polun, esimerkiksi **\\V2\PROFILES\ALL\PROGRAMS**

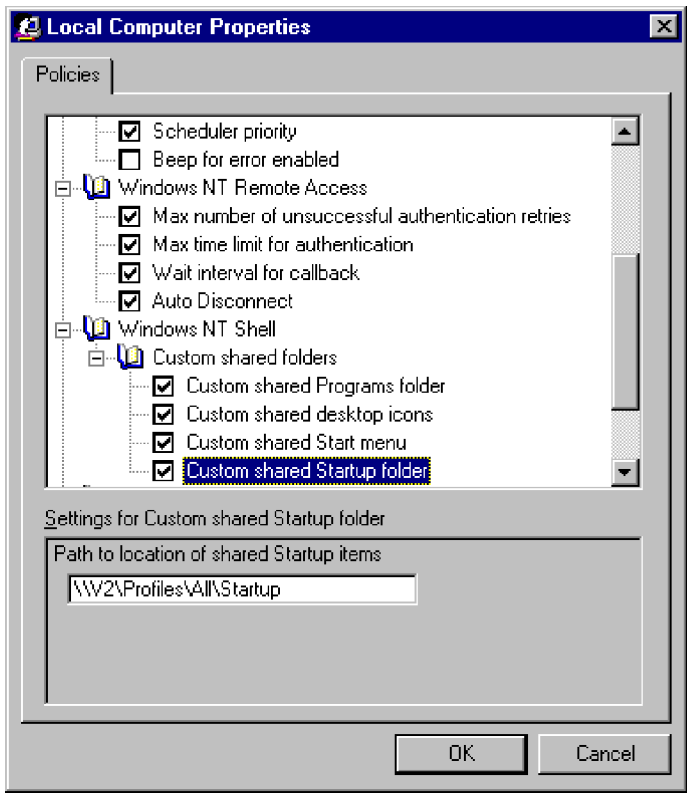
- **Custom shared desktop icons**- oletuksena työpöytä viittaa polkuun **%SystemRoot%\Profiles\All Users\Desktop**. Muuttamalla asetusta **työpöytää** ei haeta All Users-profiilihakemistosta. Voit antaa **UNC**-polun, esimerkiksi **\\V2\PROFILES\ALL\DESKTOP**

- **Custom shared Start menu** - oletuksena käynnistyvalikko viittaa polkuun **%SystemRoot%\Profiles\All Users\Start Menu**.

Tähänkin voi **antaa** haluttaessa antaa jonkin muun polun, vaikkapa verkon palvelimen hakemiston **UNC**-polkuna, esimerkiksi **\\V2\PROFILES\ALL\START**

- **Custom Startup folder** - oletuksena automaattisesti käynnistettävien sovellusten kansio viittaa polkuun **%SystemRoot%\Profiles\All Users\Start Menu\Programs\Startup**. Tähän voi haluttaessa antaa jonkin muun, vaikkapa verkon palvelimen hakemiston UNC-polkuna, esimerkiksi **\\V2\PROFILES\ALL\STARTUP**.

Esimerkki: kaikille käyttäjille yhteiset käynnistysvalikon osat haetaan palvelimelta.



Valitut asetukset ovat:

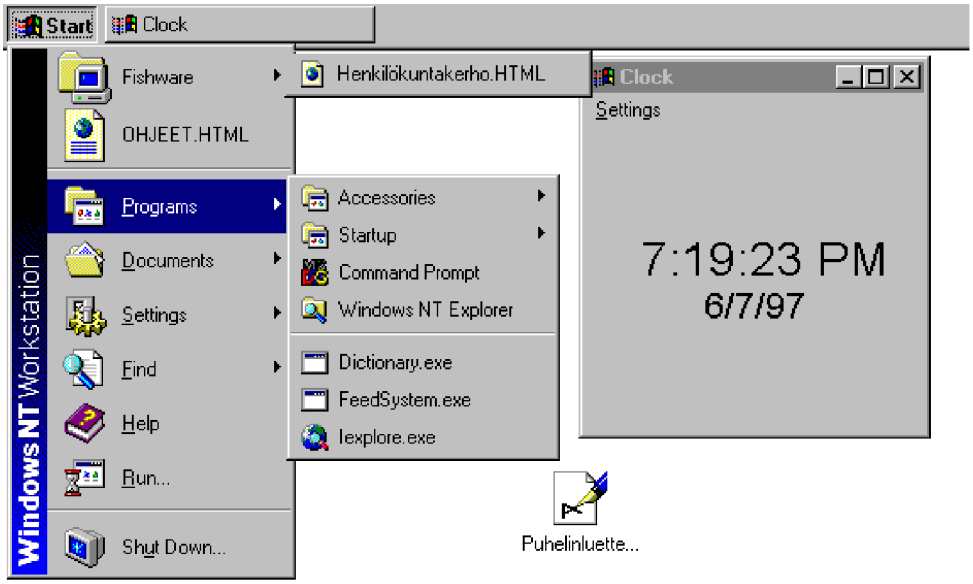
- Custom shared Programs folder - \\V2\PROFILES\ALL\PROGRAMS
- Custom shared desktop icons - \\V2\PROFILES\ALL\DESKTOP
- Custom shared Start menu - \\V2\PROFILES\ALL\START
- Custom Startup folder - \\V2\PROFILES\ALL\STARTUP.

UNC-polut ja hakemistojen sisältö esimerkissä on seuraava:

UNC-polku	Sisältö
\\V2\PROFILES\ALL\PROGRAMS	Iexplore.exe, Dictionary.exe, Feedsystem.exe
\\V2\PROFILES\ALL\DESKTOP	Puhelinluettelo.txt
\\V2\PROFILES\ALL\STARTUP	Clock.exe
\\V2\PROFILES\ALL\START	Fishware-kansio, OHJEET.HTML

Korvaa esimerkin hakemistot ja kuvakkeet omaan ympäristöösi sopiviksi.

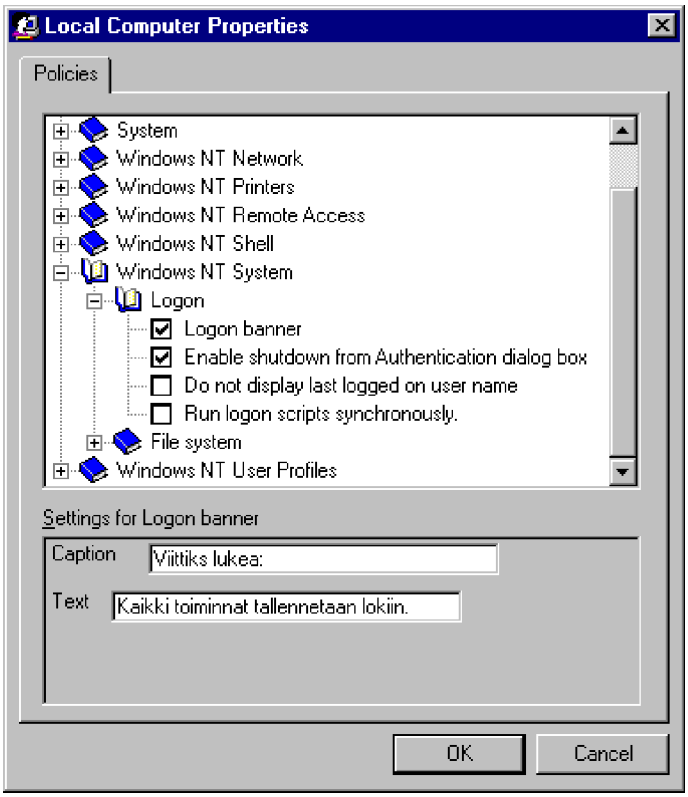
Käyttäjän kirjautuessa ympäristö näyttää tältä:



Kello käynnistyy, työpöydältä löytyy **Puhelinluettelo**, käynnistysvalikosta **Fishware**-valinta (jossa **Henkilökuntakerho.HTML**) ja **OHJEET.-HTML**. Lisäksi **Programs**-valikosta löytyy **Iexplore.exe**, **Dictionary.exe** ja **Feedsystem.exe**.

Windows NT System

Windows NT Systemissä voidaan asettaa kaikki NT-konetta käyttäviä koskevia kirjautumissääntöjä.



Logon:

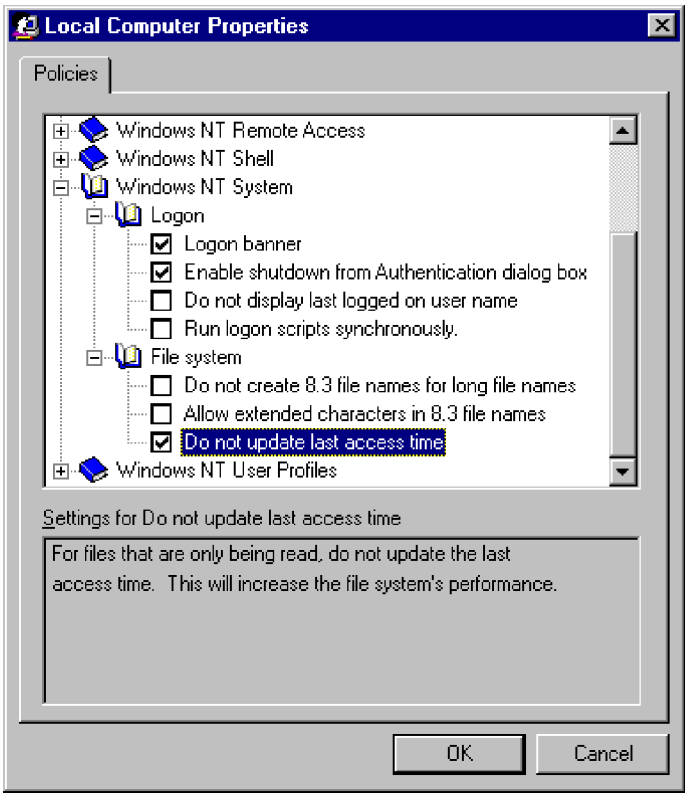
- **Logon banner** on kirjautumisessa näyttöön tuleva ikkuna, joka on hyväksyttävä OK:lla. Anna otsikko ja teksti

- **Enable shutdown from Authentication dialog box** - valitse tai estä Welcome-ikkunan Shut down -painikkeen käyttö. Jos käyttö estetään, varmistetaan, että luvaton käyttäjä ei voi sammuttaa järjestelmää

- **Do not display last logged on user name** - ei näytetä edellisen kirjautuneen käyttäjän tunnusta

- **Run Logon scripts synchronously** - tällä valinnalla ensin suoritetaan kirjauskomentojono, sitten vasta tulee käyttöliitymä käytettäväksi.

File System:

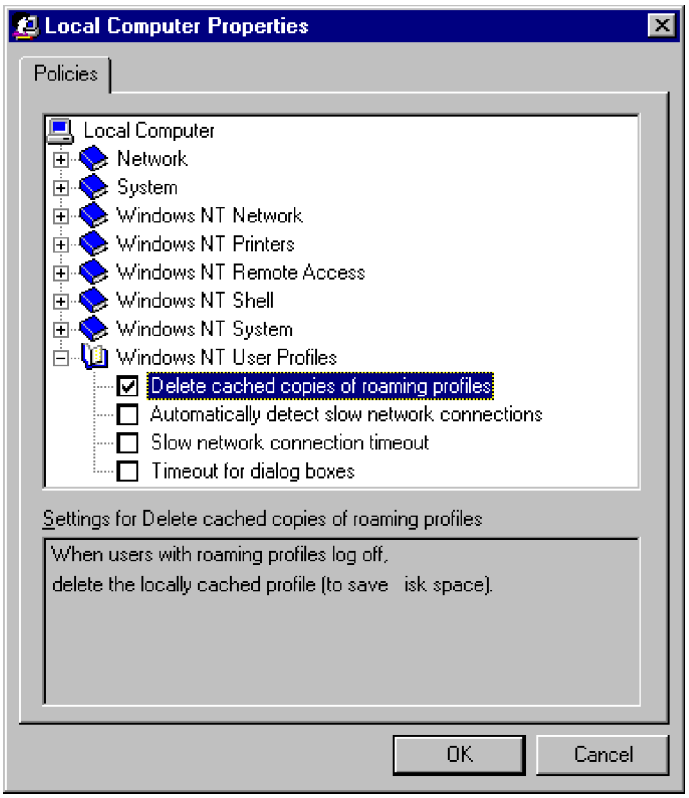


Valinnat ovat:

- **Do not create 8.3 file names for long file names** - ei luoda MS-DOS-yhteensopivia tiedostonimiä
- **Allow extended characters in 8.3 file names** - sallitaanko erikoismerkkejä lyhyissä MS-DOS-yhteensopivissa tiedostonimissä
- **Do not update last access time** - päivitetäänkö myös tiedostoa luettaessa merkintä tiedoston viimeiseen käyttöön. Jos ei, niin levyn käyttö nopeutuu.

Windows NT User Profiles

Näillä asetuksilla määritellään profiilien käsittely.



Valinnat ovat:

- **Delete cached copies of roaming profiles** - poistetaan NT-työaseman kiintolevyltä palvelimella sijaitsevan profiilin kopio - hyödyllinen! Säästää levytilaa ja lisää tietoturvallisuutta

- **Automatically detect slow network connections** - hitaiden verkkoyhteyksien tunnistaminen. Tilanteesta riippuen käyttäjältä kysytään mitä tilanteessa tehdään

- **Slow network connection timeout** - kauanko esimerkiksi verkkoasemaa yritetään palauttaa hitaan verkkoyhteyden kautta

- **Timeout for dialog boxes** - odotusaika käyttäjän vastauksille.

Paikallisen rekisterin käsittely

Voit käyttää System Policy Editoria kahdessa eri tilassa:

- Työaseman **paikallisen rekisterin** tai **etähallitun työaseman rekisterin** käsittelyssä. Tällöin asetukset menevät samantien kyseisen työaseman rekisteriin! Tällöin käsitellään paikallisen rekisterin asetuksia. Kyseinen työasema on käynnistettävä uudelleen, jotta asetukset tulevat voimaan

- **Järjestelmäkäytäntötiedostojen** (.**POL**) muokkaamiseen. Näitä voit luoda aivan vapaasti, mutta suosittelen noudattamaan Windows NT:n oletuksia! Tämä on ns. *Policy File Mode*.

Voit asentaa System Policy Editorin myös Windows NT 4.0-työasemaan. Asentaminen onnistuu Windows NT 4.0 -palvelimen CD-ROM:ilta **Clients\Srvtools\Winnt**-kansiosta komennolla **SETUP**.

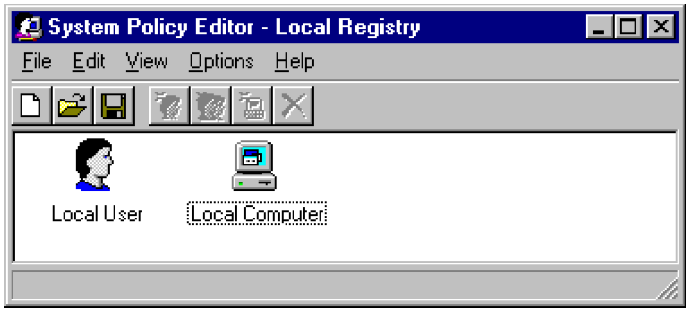
Työaseman **paikallisen rekisterin** tai **etähallitun työaseman rekisterin** käsittelyssä toimitaan seuraavasti:

1) Valitse **File** | **Open Registry**. Jos haluat avata toisen työaseman rekisterin, valitse **Connect** ja anna toisen työaseman nimi

2) Näyttöön tulee paikallinen rekisteri oletuskäyttäjineen (**Local User**, **Local Computer**).

3) Tee halutut asetukset ja tallenna tiedosto. Muutokset kirjoitetaan tehdään **välittömästi rekisteriin**, kun valitse **File** | **Save**.

Asetukset tulevat voimaan työaseman käyttäjille joko uudelleenkirjautumisen tai uudelleenkäynnistyksen jälkeen.

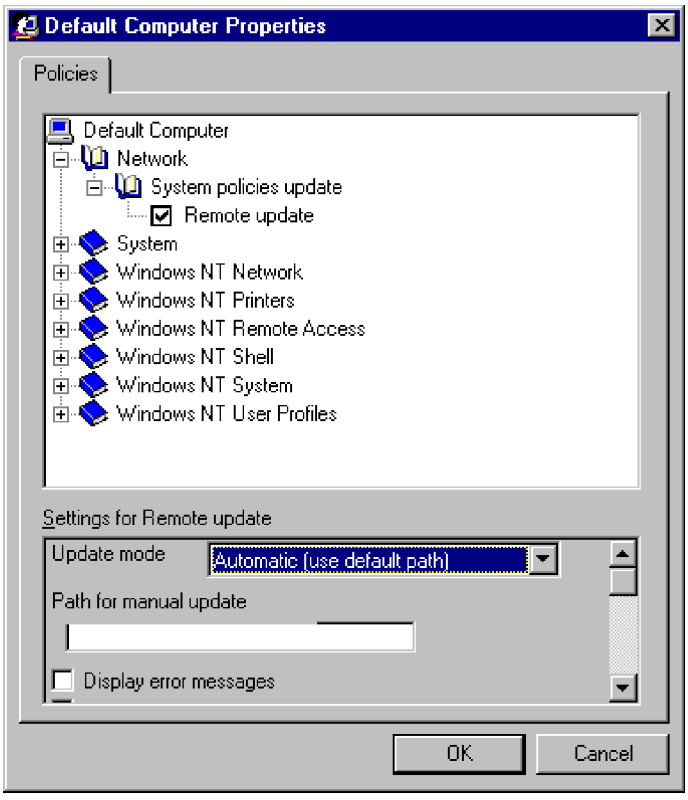


NTConfig.pol-järjestelmäkäytäntötiedosto

NTConfig.POL-tiedosto on järjestelmäkäytäntötiedosto, jonka Windows NT 4.0 osaa lukea verkon palvelimelta automaattisesti. Oletuksena lataus tapahtuu Windows NT -palvelimen **NETLOGON** -hakemistosta.

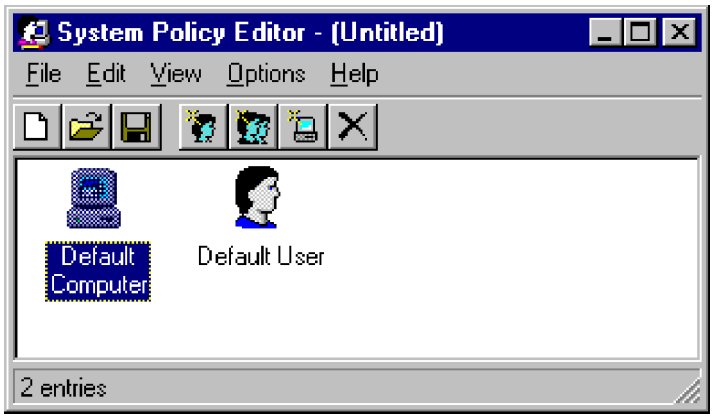
Käyttäjällä, käyttäjäryhmällä ja työasemalla voi olla omat asetuksensa. Ne voidaan tallentaa suoraan **NTConfig.POL**-tiedostoon. Jos tiedosto löytyy, sen sisältö kopioidaan paikallisen NT-koneen rekisteriin, ja sillä korvataan rekisterin senhetkiset käyttäjää ja paikallista NT-konetta koskevat osat.

Työasemissa on oltava käytössä **Automatic**-päivitysmenettely! Lue aiemmin tässä luvussa esitelty järjestelmäkäytäntöjen periaate.



NTConfig.POL-järjestelmäkäytäntötiedoston luomisessa toimitaan seuraavasti:

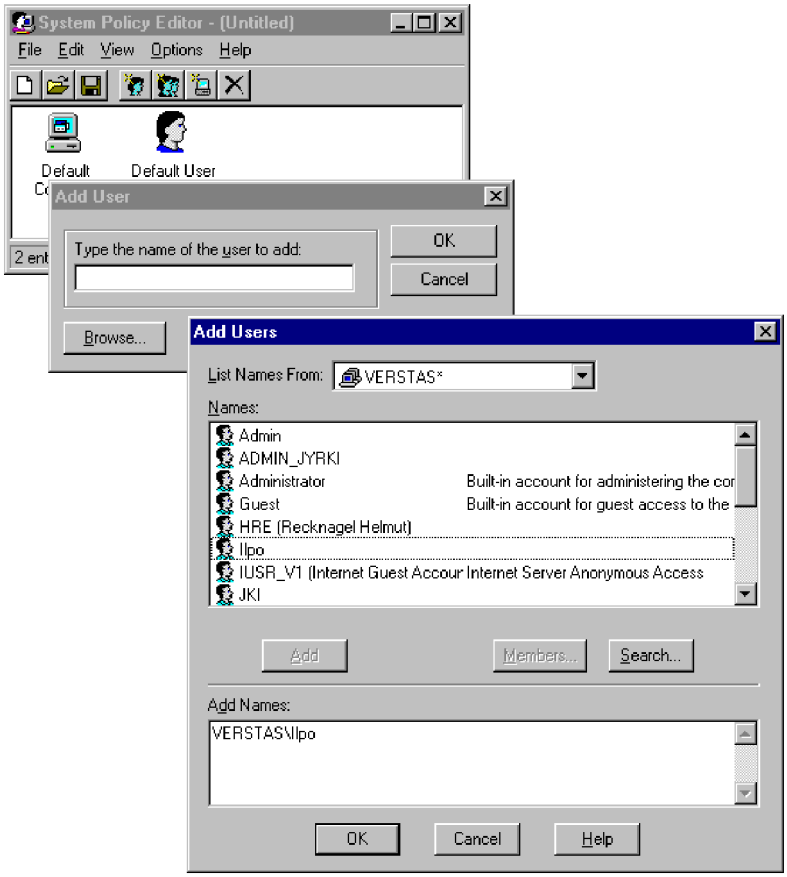
1) Valitse **File** | **New Policy**



2) Näyttöön tulee oletusympäristön asetukset (**Default Computer**, **Default User**). Voit tehdä myös näihin muutoksia.

Jos käyttäjällä tai käyttäjän ryhmällä **ei** ole asetuksia, **Default User**in asetuksia käytetään! Samoin on työaseman asetusten laita.

Jos haluat määritellä **yksittäiselle käyttäjälle** asetuksia:



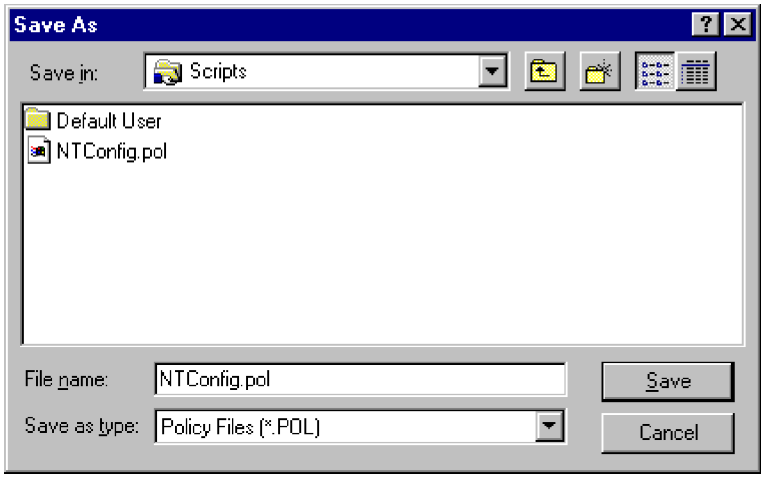
Valitse **Edit** | **Add User**. Anna käyttäjätunnus tai paina **Browse**, jolloin voit selata toimialueen käyttäjätunnuksia.

Paina lopuksi **OK**. Käyttäjätunnus tulee näkyviin, ja voit kaksoisnapauttamalla siirtyä käsittelemään käyttäjän asetuksia.

Jos haluat määritellä **käyttäjäryhmän** asetuksia, valitse **Edit** | **Add Group**. Anna ryhmän nimi tai paina **Browse**, jolloin voit selata toimialueen käyttäjäryhmiä. Paina lopuksi **OK**. Käyttäjäryhmä tulee näkyviin, ja voit kaksoisnapauttamalla siirtyä käsittelemään käyttäjäryhmän asetuksia.

Jos haluat määritellä **NT-koneen** asetuksia, valitse **Edit** | **Add Computer**. Anna NT-koneen nimi tai paina **Browse**, jolloin voit selata toimialueen NT-koneiden tunnuksia. Paina lopuksi **OK**. NT-koneen tunnus tulee näkyviin, ja voit kaksoisnapauttamalla siirtyä käsittelemään NT-koneen asetuksia.

3) Tee halutut asetukset ja tallenna tiedosto valitsemalla **File** | **Save**.



Tallenna tiedosto nimellä **NTConfig.pol** PDC:n **NETLOGON**-jakoon (hakemisto on **Winnt\System32\Repl\Import\Scripts**).

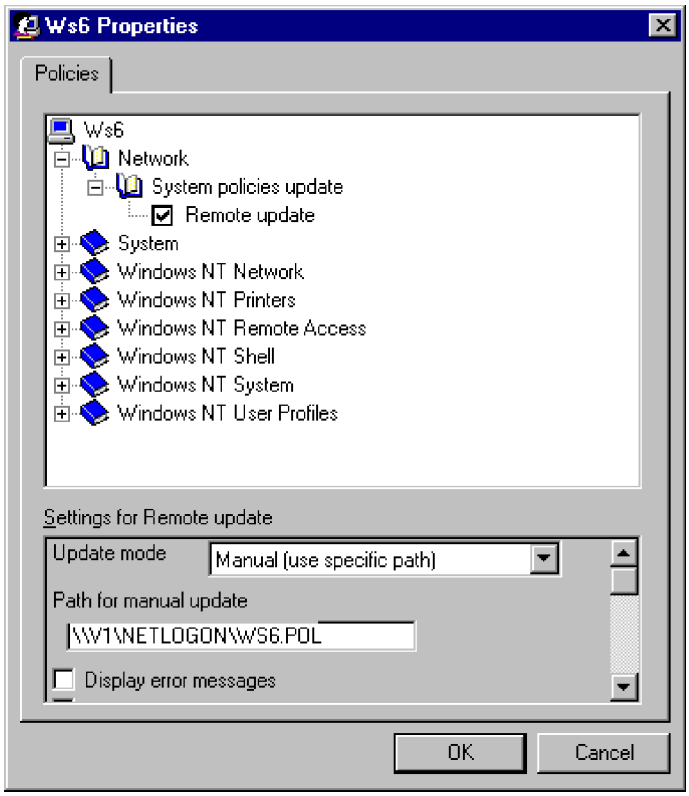
Huomaa, että verkon kautta **NETLOGON**-jakoon on oletuksena vain lukuoikeudet! Testaa tämän jälkeen asetukset ja tee tarvittaessa muutokset **NTConfig.pol** -tiedostoon.

Erilliset järjestelmäkäytäntötiedostot

Voit myös luoda järjestelmäkäytäntötiedostoja, jotka otetaan käyttöön UNC-polun takaa ns. **manuaalisella päivityksellä**.

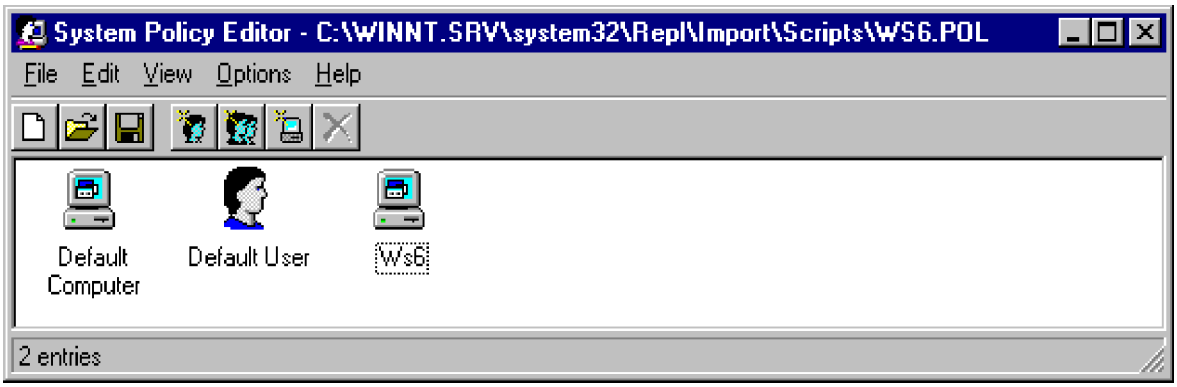
Valitse tällöin **Update mode**ksi voi **Manual**. Automatic käyttää **NETLOGON**-jakoa ja **NTConfig.pol**-tiedostoa ja se on oletuksena käytössä.

Kun valitset **Manual**, anna myös **Path for manual update**: tämä on polku järjestelmäkäytäntötiedostoon.



Polku voi olla paikallinen hakemisto ja tiedosto, esimerkiksi **C:\Winnt\WS6.POL** tai UNC-nimi, esimerkiksi **\\P1\Profiles\WS6.POL**.

Toki nämäkin tiedostot voivat sijaita **NETLOGON**-jaossa.



6. PALVELIMEN VALVONTA-TYÖKALUT

Windows NT -palvelimessa käytettävissä olevien valvontatyökalujen (Administrative Tools) valikoima riippuu osittain palvelimeen asennetuista palveluista. Keskeiset valvontatyökalut on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

Tässä luvussa esitellään palvelimen kaikki valvontaohjelmat vain lyhyesti. Tärkeimmistä työkaluista mainitaan viitteet muualla tässä kirjassa.

Palvelimen ja työaseman valvontatyökalujen erot

Kannattaa muistaa, että osalla Windows NT -työaseman valvontatyökaluista voit valvoa myös NT-palvelimia tai mitä tahansa NT-työasemia omasta työasemastasi käsin. Windows NT -palvelimen ja -työaseman yhteiset valvontatyökalut ovat seuraavat:

- **Etäkäytön hallinta** (Remote Access Admin), jonka avulla voit hallita myös NT-palvelimen tai minkä tahansa NT-työaseman etäkäyttöpalvelua työasemasta
- **Käyttäjien hallinta** (User Manager)
- **Levynhallinta** (Disk Administrator)
- **Resurssien valvonta** (Performance Monitor), jonka avulla voit seurata myös NT-palvelimen tai minkä tahansa NT-työaseman suorituskykyä työasemasta
- **Tapahtumien valvonta** (Event Viewer), jonka avulla voit seurata NT-palvelimen tai minkä tahansa NT-työaseman tapahtumalokia työasemasta

- **Varmuuskopiointi** (Backup) - NT-palvelimen tai minkä tahansa NT-työaseman levyasemien varmistuskopiointiin - et voi kuitenkaan varmistaa toisen NT-koneen rekisteriä verkon yli tämän avulla

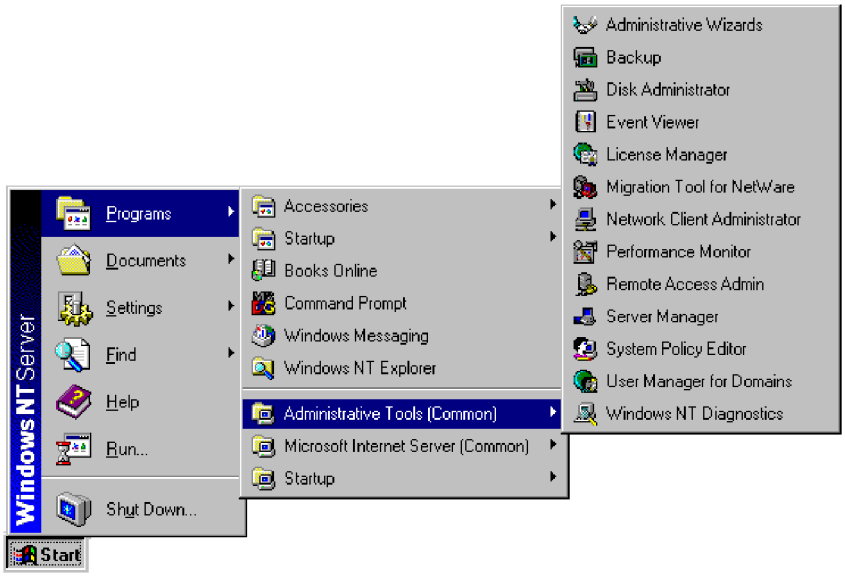
- **Windows NT Diagnostiikka** (Windows NT Diagnostics), jonka avulla voit seurata myös NT-palvelimen tai minkä tahansa NT-työaseman laitteistoasetuksia omasta työasemastasi.

Näiden Windows NT -palvelimen ja -työaseman yhteisten valvontatyökalujen erot ovat seuraavat:

- Palvelimen valvontatyökalujen kokoelma sisältää esimerkiksi toimialueen käyttäjien hallinnan **User Manager for Domains**, kun työasema sisältää vain **Käyttäjien hallinnan** (User Manager). Palvelimen versiossa on siis koko toimialueen käyttäjien hallinta, työasemaversiossa vain yksittäisen NT:n työaseman käyttäjien hallinta.

- Palvelimen **Disk Administrator** sisältää vikasietoisuuslaajennukset, jotka NT-työasemaversiosta puuttuvat.

- Palvelimessa on myös palvelimen hallinta **Server Manager** sekä järjestelmäkäytäntöjen editori **System Policy Editor**, jotka puuttuvat työasemaversiosta.



Windows NT -palvelimen valvontatyökalut

Lisäksi Windows NT 4.0 -palvelimessa on oletuksena mukana mm. seuraavat valvontatyökalut:

- **Administrative Wizards** - valvontatyökalujen velhot
- **License Manager** - lisenssien valvonta
- **Migration Tool For NetWare** - Novell NetWaren integrointityökalut
- **Network Client Administrator** - työasemien asennuslevykkeiden ja Windows 95-työasemien asentaminen verkon yli
- **Server Manager** - palvelimen hallinta
- **System Policy Editor** - järjestelmäkäytäntöjen editori
- **User Manager for Domains** - toimialueen käyttäjien hallinta.

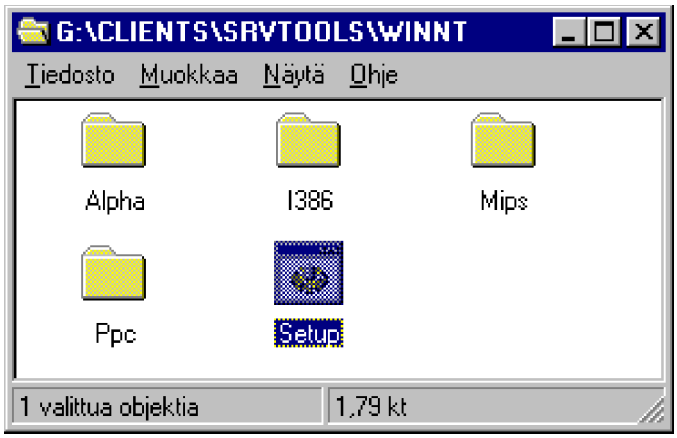
Seuraavat valvontatyökalut riippuvat palvelimeen asennetuista palveluista:

- **DHCP Manager** - DHCP-palvelimen hallinta
- **DNS Manager** - DNS-palvelimen hallinta
- **WINS Manager** - WINS-palvelimen hallinta.

Palvelimen valvontatyökalujen asentaminen työasemaan

Tarpeellisimpien valvontatyökalujen eli toimialueen käyttäjien hallinnan **User Manager for Domains** ja palvelimen hallinnan **Server Manager** sekä järjestelmäkäytäntöjen editorin **System Policy Editor** Windows 95- ja Windows NT 4.0 -työasemaversiot tulevat Windows NT 4.0 -palvelimen CD-ROM:in mukana. **CLIENTS\SRVTOOLS**-hakemistosta on asennettavissa myös työasemaversiot RAS-, WINS-, DHCP- ja RPL-hallintasovelluksille.

Windows NT 4.0 Serverin CD-ROM:illa tulevat **Windows NT 4.0** -työasemaversiot hallintasovelluksista. Windows NT:n hallintaohjelmien NT-työasemaversion asennus tehdään siirtymällä NT 4.0 Server -CD-ROM:in **CLIENTS\SRVTOOLS\WINNT**-hakemistoon ja käynnistämällä asennusohjelma **SETUP**:

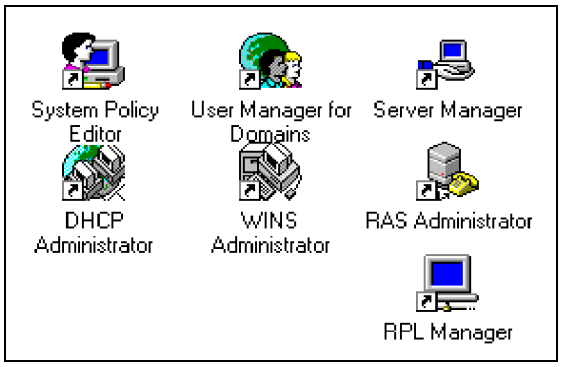


Jos asennat ohjelmat esimerkiksi verkkoon jaetusta CD-ROM:ista tai -hakemistosta, ota resurssi ensin käyttöön levyasematunnuksena! Asennusohjelma ei tue UNC-nimiä!

Asennusohjelma **ei tee** kuitenkaan kuvakkeita automaattisesti, vaan seuraavat kuvakkeet on itse lisättävä: todennäköisimmin ne löytyvät **C:\WINNT\SYSTEM32**-hakemistosta:

Ohjelmatiedosto	Kuvaus
SRVMGR.EXE	Server Manager
USRMGR.EXE	User Manager For Domains
DHCPADMN.EXE	DHCP Administrator
RASADMIN.EXE	Remote Access Service Manager
RPLMGR.EXE	Remote Boot
POLEDIT.EXE	System Policy Editor
WINSADMN.EXE	WINS Admin

Voit tehdä hallintaohjelmista vaikkapa pikakuvakkeet työpöydällesi:



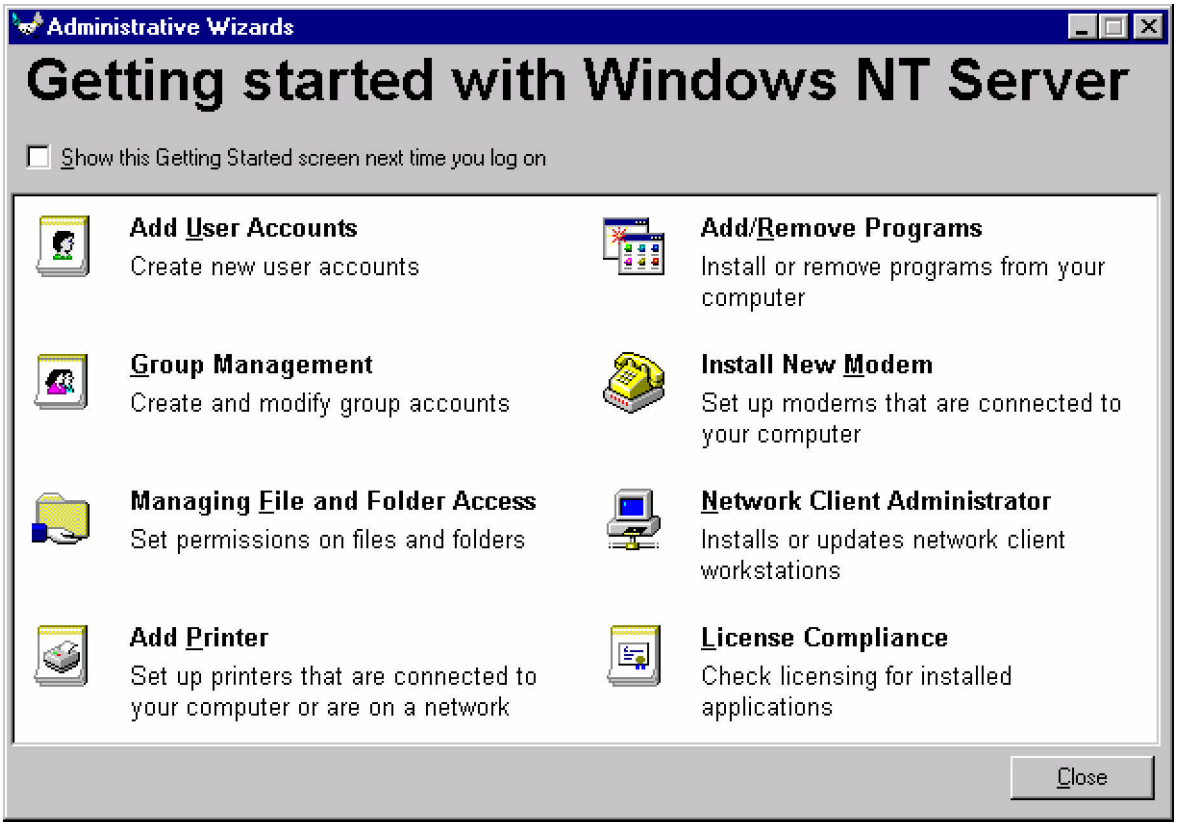
Lisää tietoturvallisuutta saat, jos suojaat NTFS-levylle kopioidut valvonta-ohjelmien ohjelmatiedostot esimerkiksi sallimalla vain pääkäyttäjille käyttöoikeudet - varmuuden vuoksi. Muilla oikeuksilla näitä ohjelmia ei muutenkaan tyypillisesti pysty suorittamaan.

Windows 95:ssä asentaminen tehdään erikseen Windows 95:n **Ohjauspaneelin** (Control Panel) **Lisää/Poista sovellus** (Add/Remove Programs)-kuvakkeen avulla.

Administrative Wizards

Valinnalla **Administrative Wizards** käynnistyy valvontatyökalujen velhot eli ohjatut toiminnot järjestelmänhallinnan rutiineille.

Kokeneempi NT-verkon tukihenkilö ei näitä tarvinne, vaan käyttää suoraan a.o. työkalua. Velhoista on kuitenkin iloa silloin, kun halutaan varmistaa että kaikki tiettyyn toimintoon liittyvät asetukset tulevat varmasti annetuiksi.



Toiminnot ovat seuraavat:

- **Add User Accounts** - käyttäjätunnusten lisääminen (ks. Luku 5)
- **Group Management** - käyttäjäryhmien hallinta (ks. Luku 5)
- **Managing File and Folder Access** - suojausasetukset (ks. Luku 11 sekä lisää suojauksista tässä luvussa)
- **Add Printer** - kirjoittimien lisääminen ja asetukset - Ohjauspaneelin **Printers** | **Add Printer** (ks. Luku 3)

- **Add/Remove Programs** - ohjelmien asentaminen ja asennettujen ohjelmien poistaminen (ks. Luku 3)
- **Install New Modem** - Ohjauspaneelin **Modems** (ks. Luku 3)
- **Network Client Administrator** - vastaava valvontatyökalu
- **License Compliance** - Ohjauspaneelin **Licensing** (ks. Luku 3).

Valvontatyökalut

Seuraavaksi listaus palvelimen valvontatyökaluista, siten kuin ne löytyvät **Start** | **Programs** | **Administrative Tools**-valikosta:

- **Backup** - Windows NT:n **Backup**-varmuuskopiointiohjelmalla voit tallentaa sekä paikallisten että verkkoasemien tiedostoja nauha-asemaan. Paikalliset levyasemat voivat käyttää NTFS- tai FAT-tiedostojärjestelmää, myös CD-ROM:in (CDFS) tiedostoja voi tallentaa. Voit myös varmistaa Backup-ohjelmaa ajavan NT-koneen rekisterin. Backup-ohjelmaa suomenkielisessä NT 4.0-työasemassa on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä. Backup-ohjelmaa ja varmistusmenetelmiä on käsitelty lisäksi luvussa **12**.
- **DHCP Manager** - DHCP-palvelimen avulla voidaan jakaa työasemille valmiiksi konfiguroituja IP-osoitteita. DHCP:n hallintaa NT 4.0-työasemasta on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä. DHCP-palvelimen hallintaa on käsitelty luvussa **8**.
- **Disk Administrator** on tehokas työkalu levyjen hallintaan, joka sisältää laajennettuina kaikki perinteisen **FDISK**-ohjelman toiminnot. Voit halutessasi muuttaa kiintolevyn osioita, osioida mikroon lisättyjä uusia kiintolevyjä tai muuttaa levyasematunnuksia. Palvelinversio sisältää myös joitakin vikasietoisuusominaisuuksia, joita voiharkinnan mukaan ottaa tarvittaessa käyttöön. Levynhallintaohjelmaa suomenkielisessa NT 4.0-työasemassa on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä. **Disk Administrator**-ohjelmaa on käsitelty luvussa **12**.

- **DNS Manager** - DNS-nimipalvelu on Windows NT 4.0 -palvelimen uusi ominaisuus. DNS-palvelimen hallintaa on käsitelty luvussa **8**.

- **Event Viewerin** avulla valvotaan NT:n tapahtumia. Voit tarkastella ja hallita **järjestelmälokeja**, **suojauslokeja** ja **sovelluslokeja** sekä tallentaa näiden muodostamia **tapahtumalokeja**. Tapahtumanvalvontaa suomenkielisessa NT 4.0-työasemassa on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä. **Event Viewer**-ohjelmaa palvelimen kannalta on käsitelty luvussa **12**.

- **License Manager** - lisenssien valvontaohjelma

- **Migration Tool For NetWare** - Novell NetWaren integrointityökalut. Novell-asioita on käsitelty luvussa **7**.

- **Network Client Administrator** - Windows 95- ja DOS-työasemien asennusohjelma. Aihetta on käsitelty luvussa **7**.

- **Performance Monitor** - järjestelmän suorituskyvyn seurantaa palvelimen kannalta on käsitelty luvussa **12**. **Resurssien valvontaa** työaseman kannalta on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

- **Remote Access Admin** - etäkäytön hallinnalla voit hallita NT-palvelimen tai minkä tahansa NT-työaseman etäkäyttöpalvelua. Katso myös luku **7**. Etäkäyttöpalvelua ja sen hallintaa työasemasta on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä**.**

- **Server Manager** - palvelimien hallinnan avulla voit hallita toimialueita ja NT- tai LAN Manager -palvelimia ja NT-työasemia. Aihetta on käsitelty luvussa **7**. Palvelimien hallintaa työasemasta on käsitelty myös **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä**.**

- **System Policy Editor** on järjestelmäkäytäntöjen editori, jolla voidaan määritellä lisäsuojauksia työasemille, yksittäisille käyttäjille tai käyttäjäryhmille tarvittaessa toimialuelaajuisesti. Aihetta on käsitelty luvussa **5**.

- **User Manager for Domains** - käyttäjien hallintaa on käsitelty luvussa **5**. **Käyttäjien hallinta**-ohjelmaa suomenkielisessä NT 4.0-työasemassa on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

- **Windows NT Diagnostics** - järjestelmän asetusten tarkastelua on käsitelty luvussa **12**. **Windows NT Diagnostiikka** -ohjelmaa suomenkielisessä NT 4.0 -työasemassa on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

- **WINS Manager** - WINS-palvelimen hallintaa ja palvelimien yhdistämistä on käsitelty luvussa **8**. WINS:in hallintaa NT 4.0 -työasemasta on käsitelty myös **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

7. VERKKOPALVELUT

Tässä luvussa käsitellään verkon palvelimien ja niiden resurssien sekä palveluiden hallintaa.

Palvelimien rooleja ja käyttäjien hallintaa on käsitelty luvussa **5**. Järjestelmän ylläpitoa käsitellään myös luvussa **12**.

Palvelimien hallinta hoidetaan tyypillisesti **Server Manager**-ohjelmalla. Muitakin välineitä on käytettävissä, ja niitäkin esitellään tässä luvussa.

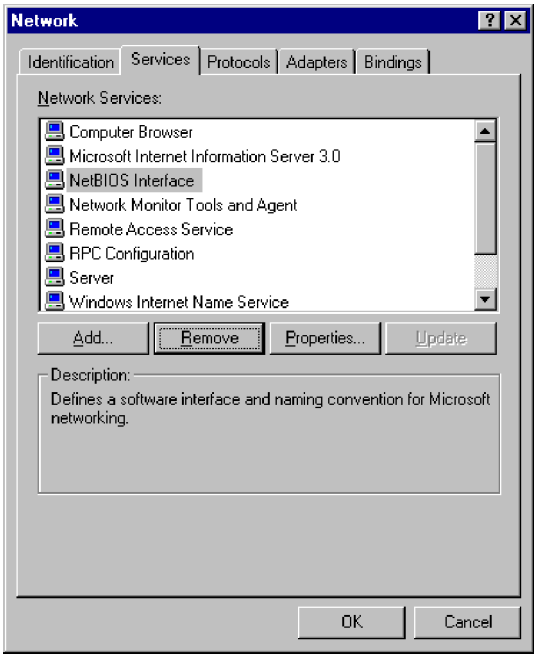
Verkkojen perusasioita on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas 1**:ssä.

Palvelimen palvelut

Ennenkuin NT-palvelimia voidaan menetyksellisesti hallita, on syytä tietää jotakin palvelimissa ajettavista palveluista.

Palveluiden lisääminen ja poistaminen

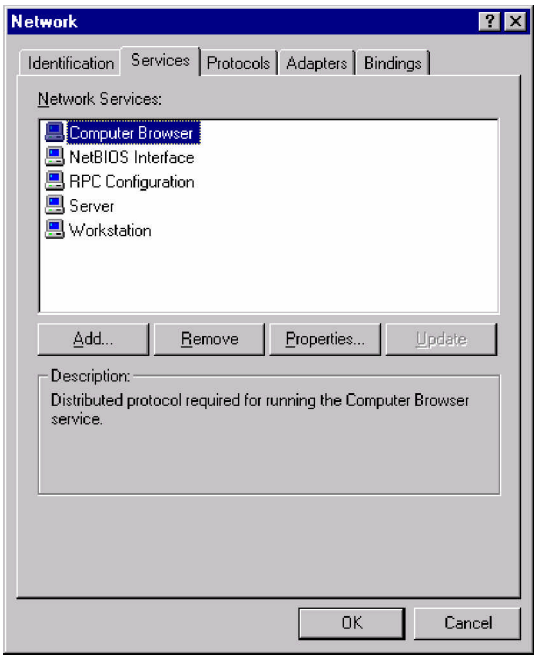
Palveluita voidaan lisätä tavallisesti Ohjauspaneelin **Network**-kuvakkeella **Services**-välilehdestä. **Add**-painikkeella voidaan selata lisättävät palvelut - valinta listaa tyypillisesti NT:n mukana tulevat palvelut.



Remove-painikkeella voidaan poistaa palveluita, mutta tällöin on syytä tietää **miksi palvelu poistetaan ja mitä sen poistaminen aiheuttaa**.

Update-painikkeella palvelu voidaan päivittää.

Palveluita voidaan lisätä joissakin tapauksissa myös Ohjauspaneelin **Add/Remove Programs**-kuvakkeella.



NT-palvelimen tarpeelliset jo asennuksen yhteydessä asennetut ja Ohjauspaneelissa määriteltävät **peruspalvelut** ovat seuraavat:

Palvelu	Kuvaus
Computer Browser	Selauspalvelu
NetBIOS Interface	NetBIOS-rajapinta; etähallinta ja NetBIOS-sovellusten (esimerkiksi NET-komennot) suoritus
RPC Configuration	Etäproseduurikutsupalvelun (RPC) -asetukset, RPC mm. mahdollistaa prosessien suorittamisen etäkoneessa
Server	Palvelimen resurssien jakamisen mahdollistava komponentti
Workstation	Työaseman verkkokäytön mahdollistava komponentti ja perusta muille palveluille

Näiden palveluiden perusteeton poistaminen voi aiheuttaa palvelimen peruspalveluiden sekä koko järjestelmän (myös muiden palvelimien) toiminnan joutumisen epävakaaseen tilaan.

Useimmat peruspalvelut voidaan konfiguroida suoraan **Services**-välilehden **Properties**-painikkeella: **Computer Browser**-, **NetBIOS Interface**-, **RPC Configuration**- ja **Server**-palvelut. Itse asiassa vain **Workstation**-palvelu ie ole konfiguroitavissa Ohjauspaneelista.

Lisättäviä palveluita ovat mm. seuraavat:

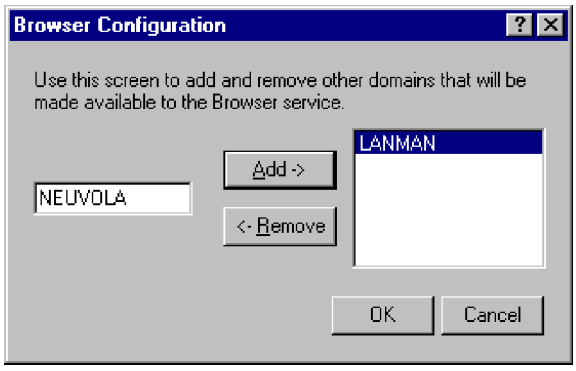
Palvelu	Kuvaus
DHCP Relay Agent	DHCP-palvelimen jakamia IP-osoitteita välityspalvelu
Gateway (and Client) Services for NetWare	Yhdyskäytävä- ja työasematuki NetWare-verkolle
Microsoft DHCP Server	IP-osoitteita jakava DHCP-palvelin
Microsoft DNS Server	DNS-nimipalvelu
Microsoft Internet Information Server	WWW-, Gopher- ja FTP-palvelin

Microsoft TCP/IP Printing	Tulostuspalvelu Unix-palvelimiin ja -työasemiin
Network Monitor Agent	Verkkomonitorin agentti
Network Monitor Tools and Agent	Verkkomonitorin työkalu ja agentti
Remote Access Service	Tuki etäkäytölle, sekä asiakas että palvelin
Remoteboot Service	Tuki levyttömille työasemille
RIP for Internet Protocol	Reitittimien käyttämän RIP (*Routing Information Protocol*)-protokollan tuki IP-protokollalle
RIP for NWLink IPX/SPX compatible transport	reitittimien käyttämän RIP-protokollan tuki IPX/SPX-protokollalle
RPC Configuration	RPC mahdollistaa prosessien suorittamisen etä-koneessa
RPC Support for Banyan	RPC-tuki Banyan Vines -verkolle
SAP Agent	SAP (*Service Advertising Protocol*) on Novellin protokolla, jolla mainostetaan Novell-palvelimen tarjoamia palveluita yleissanomien (*broadcast*) avulla. SAP-agentti osaa välittää näitä yleis-sanomia
Services for Macintosh	Palvelimen Macintosh-tuki
Simple TCP/IP Services	TCP/IP-apuohjelmat
SNMP Service	SNMP (*Simple Network Management Protocol*) tarjoaa SNMP-hallintatuen
Windows Internet Name Service	NetBIOS-nimipalvelu

Näiden palveluiden konfigurointi ja hallinta voidaan tyypillisesti hoitaa joko Ohjauspaneelin erillisillä kuvakkeilla tai palvelun asentamisen myötä asennettavilla valvontatyökaluilla.
SNMP- ja **Remote Access Service** -palvelut voidaan konfiguroida suoraan **Services**-välilehden **Properties**-painikkeella.

Computer Browser

Computer Browser -selauspalvelu pitää luetteloa toimialueista/työryhmistä sekä toimialueen/työryhmän työasemista/palvelimista ja se voidaan asettaa pitämään listaa myös LAN Manager-toimialueista.



Käytä selauspalvelun configurointia seuraavasti:

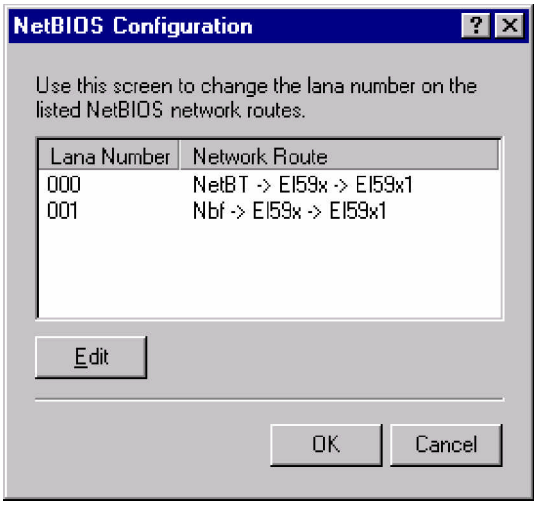
- Kirjoita selauspalveluun liitettävän toimialueen nimi ja paina **Add**. Tarvittaessa voit poistaa toimialueen selailun valitsemalla sen nimen listasta ja painamalla **Remove**

- Voit lisätä reitinverkoissa myös toisten toimialueiden nimiä, joiden työasemia tai palvelimia **ei** ole palvelimen kanssa samassa aliverkossa.

Itse verkon selauspalvelua on käsitelty tässä luvussa enemmän hieman edempänä.

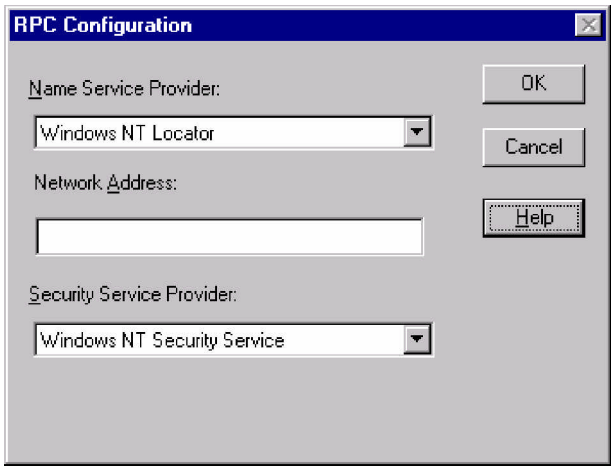
NetBIOS Interface

NetBIOS Interface -liittymän **LANA** (*LAN Adapter*) -asetuksia voit muuttaa tarvittaessa, esimerkiksi *jos* jokin sovellus *nimenomaan* vaatii jonkin tietyn LANA-numeron. Esimerkiksi kahden verkkokortin ja kahden protokollan tapauksessa on käytettävissä neljä LANA:a.



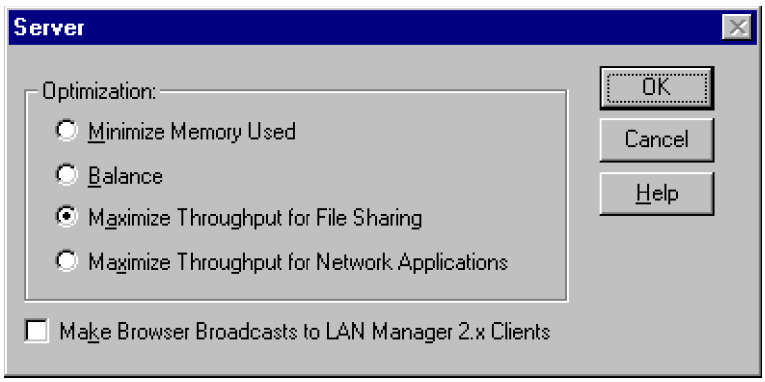
RPC Configuration

RPC:n nimipalvelutoimittajana **Name Service Provider** on oletuksena **Windows NT Locator**. Jos valitset **DCE Cell Directory -palvelun** voit asettaa myös verkko-osoitteen ja samalla voit asettaa suojauspalvelutoimittajan **Security Service Provider**.



Server

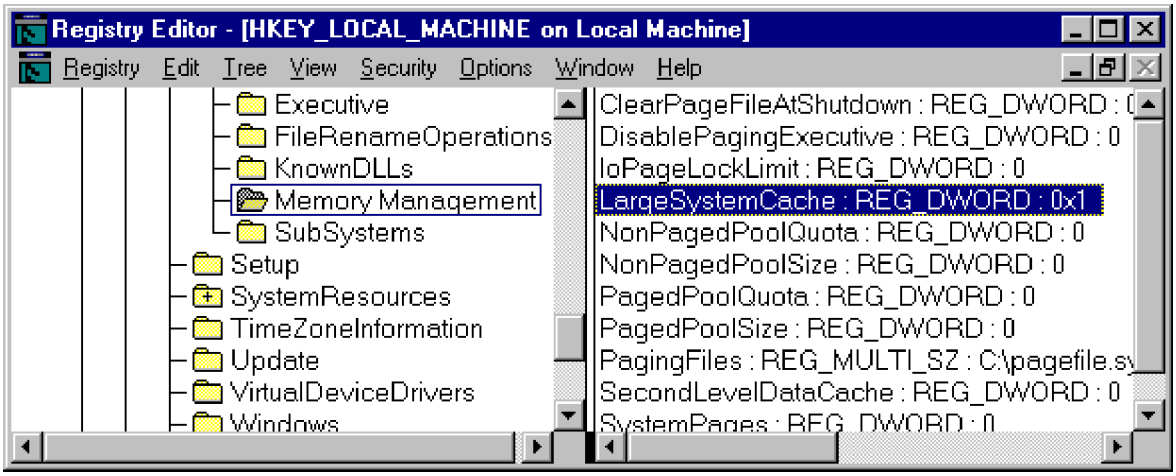
Palvelinpalvelun asetuksissa voit muuttaa verkkoyhteyksille ja käynnistetyille sovelluksille varattavan muistin määrää sekä lisäksi hallita yhteyksiä verkon LAN Manager-version 2.x -palvelimille. Voit asettaa jonkin seuraavista asetuksista:



- **Minimize Memory Used** - yhteyksiä on enintään 10 kpl
- **Balance** - yhteyksiä on enintään 64 kpl (myös NetBEUI:n oletusasetus)
- **Maximize Throughput for File Sharing** - tiedostojen jakotoiminnot saavat enemmän aikaa - tällöin tietostojärjestelmän välimuisti saa korkeamman prioriteetin ja enemmän keskusmuistia käyttöönsä
- **Maximize Throughput for Network Applications** - valitse, jos palvelimessa on esimerkiksi tietokantapalvelin, kuten **SQL Server**. Tällöin prosessit saavat korkeamman prioriteetin ja enemmän keskusmuistia käyttöönsä
- **Make Browser Broadcasts to LAN Manager 2.x Clients** - yleissanomien lähetys LM-tyyppisesti - valitse, jos haluat, että LM-palvelimet ja työasemat voivat selata NT-mikroja.

Nämä asetukset merkityksineen ovat rekisterissä seuraavat:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Control\SessionManager \MemoryManagement**
Nimi	**LargeSystemCache**
Tyyppi	**REG_DWORD**
Arvo	Määritteleekö, saako tiedostojärjestelmän välimuisti vai prosessien suoritus (working set) enemmän keskusmuistia käyttöönsä: **0** - Minimize memory used (oletus) **1** - Balance (molemmilla sama prioriteetti) **2** - Maximize throughput for file sharing (välimuisti saa korkeamman prioriteetin) **3** - Maximize throughput for network applications (prosessien suoritus saa korkeamman prioriteetin)



Asetukseen vaikuttaa myös toinen rekisterin asetus, **Size**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\LanmanServer\Parameters**
Nimi	**Size**
Tyyppi	**REG_DWORD**
Arvo	**1, 2, 3**

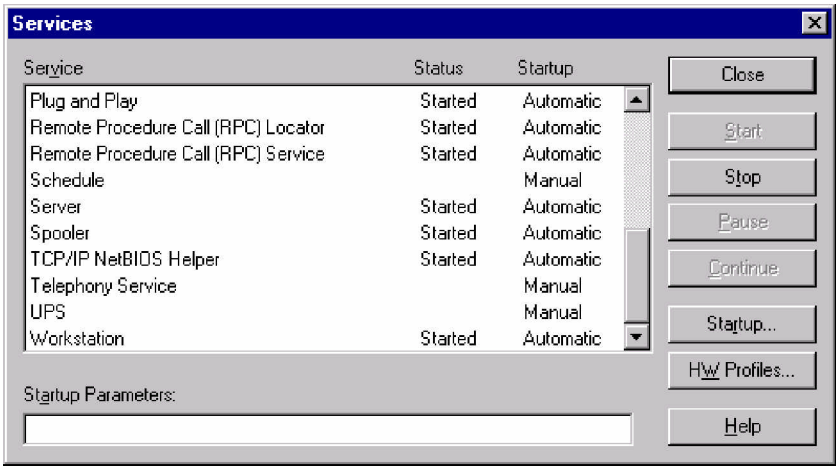
Koska palvelinpalvelun asetuksia ei ole annettavissa NT-työasemassa, voidaan tarvittaessa käyttää optimointiasetuksia NT-työasemassa seuraavasti:

Asetus	LargeSystemCache	Size
Minimize Memory Used	0	1
Balance	0	2
Maximize Throughput for File Sharing	1	3
Maximize Throughput for Network Applications	0	3

Palveluiden hallinta

Näet osan verkkopalveluista myös Ohjauspaneelin **Services**-kuvakkeessa. **Services** on palveluiden hallinta. Sillä voi lopettaa, aloittaa, keskeyttää tai jatkaa palvelimessa käytettävissä olevia palveluja, antaa niille käynnistysparametreja ja määrittää palvelujen käynnistysasetukset.

Nämä asetukset ovat myös etähallittavissa **Server Managerilla**.



Palveluiden hallinta on mahdollista myös komentorivin **NET START-** ja **NET STOP** -komennoilla. Etähallinta on mahdollista Resource Kitin **NETSVC**-ohjelmalla.

Server-palvelinpalvelun pysäyttäminen katkaisee kaikkien verkkokäyttäjien yhteyden tietokoneeseen. Varoita käyttäjiä, ennen kuin pysäytät palvelun.

Windows NT-palvelimen mukana tulevat palvelut (kaikki eivät välttämättä ole käynnistettyjä) ovat konfiguraatiosta riippuen seuraavat:

Palvelu	Kuvaus
Alerter	Hälytyspalvelu. Messenger-palvelun avulla NT-palvelimen hälytykset voidaan ohjata verkon NetBIOS-nimelle
ClipBook Server	Leikekirjapalvelin on erikseen käynnistettävä palvelimessa. **Edit** | **Copy** / **Edit** | **Paste**- ja leikekirjan tarkastelu **Clipbook Viewer** käyttää tätä palvelua
Computer Browser	Selauspalvelun ainakin palvelimissa syytä olla käytössä, jotta selauspalvelu toimii ja työasemissa voi selata verkkoa
DHCP Client	Tarvittaessa NT-kone saa DHCP:n avulla IP-osoitteen ja -asetukset. Palvelimissa tulisi välttää DHCP:llä haettuja osoitteita!
Directory Replicator	Hakemiston monistuspalvelu, erikseen käynnistettävä - kuitenkin vain jos NT-kone osallistuu monistukseen
EventLog	Tapahtumaloki - käynnistyy automaattisesti, tallentaa tapahtumalokia. Palvelua ei voi pysäyttää
FTP Publishing Service	Internet Information Server-palvelimen FTP-palvelin
Gopher Publishing Service	Internet Information Server-palvelimen Gopher-palvelin
License Logging Service	Lisenssien hallintapalvelu
Messenger	Viestinvälityspalvelu, jonka avulla NT-kone voi lähettää ja vastaanottaa sanomia. Sanoma tulee näyttöön vain, jos käyttäjä on kirjautunut NT-koneeseen ja jos Workstation-palvelu on käynnissä. Sanomat ohjataan NetBIOS-nimien avulla

Microsoft DHCP Server	DHCP-palvelin, jos asennettu
Microsoft DNS Server	DNS-palvelin, jos asennettu
MSMSQLServer	SQL Server-tietokantapalvelin, jos asennettu
Net Logon	Kirjautumispalvelu; palvelimissa **syytä** olla käytössä, jotta käyttäjien verkkoonkirjautuminen toimii! Hallitsee myös käyttäjätietokannan päivittämistä toimialueen ohjauskoneiden välillä. NT-työasemien toimialueelle kirjautuminen hoidetaan NT-työaseman Net Logon-palvelun avulla
Network DDE	Verkko-DDE (*Dynamic Data Exchange*), erikseen käynnistettävä). Käyttää NetDDE DSSM-palvelua
Network DDE DSDM	NetDDE DSSM (*DDE share database manager*), erikseen käynnistettävä
Network Monitor Agent	Verkkomonitorin agentti, erikseen asennettava ja käynnistettävä
NT LM Security Support Provider	NT LM suojausjärjestelmä niille RPC-ohjelmille, jotka käyttävät tiedonsiirtoon muita kuin nimettyjä putkia (Named Pipes). Käynnistetään automaattisesti tarvittaessa
OLE	OLE-palvelu (*Object Linking and Embedding*), erikseen käynnistettävä
Plug and Play	Kytke-ja-käytä-tuki, käynnistetään automaattisesti tarvittaessa
Remote Access Autodial Manager	Puhelinyhteyksien automaattinen avaus, käynnistetään automaattisesti tarvittaessa
Remote Access Connection Manager	Puhelinyhteyspalvelu, käynnistetään automaattisesti tarvittaessa
Remote Access Server	Etäkäyttöpalvelin, käynnistetään automaattisesti
Remote Procedure Call (RPC) Locator	Etäproseduurikutsujen (RPC) paikannin
Remote Procedure Call (RPC) Service	Etäproseduurikutsujen (RPC) palvelu
RIP for Internet Protocol	RIP-palvelu IP-protokollalle

Schedule	Ajoituspalvelu, erikseen käynnistettävä - jos esimerkiksi halutaan käyttää AT-komentoa
Server	Palvelimissa syytä olla käytössä, jotta palvelinpalvelu toimii. Käyttää SMB (Server Message Block)-palvelua
Simple TCP/IP Services	Jos asennettu, niin echo, discard jne käytettävissä
SNMP	SNMP-palvelu
SNMP Trap Service	SNMP-hälytykset
Spooler	Tulostuspalvelu - sekä tulostuspalvelin että sovellukset tulostavat tämän avulla
TCP/IP NetBIOS Helper	Jos TCP/IP on käytössä, mahdollistaa NetBIOS-rajapintaa käyttävät verkkopalvelut
Telephony Service	Puhelinyhteyspalvelu (jos asennettu) - RAS- ja DialUp-Networking käyttää
UPS	Jos UPS on kytketty, tarkkailee UPS-laitteen signaaleja
Windows Internet Name Service	WINS-palvelin (jos asennettu)
Workstation	Työasemapalvelu (Redirector), syytä olla käytössä myös palvelimissa, jotta muuta palvelut toimivat. Ohjaa muiden kuin paikallisten resurssien käsittelypyynnöt verkkoon
World Wide Web Publishing Service	Internet Information Server-palvelimen WWW-palvelin (jos asennettu)

Vaikka palveluita voikin olla käytettävissä melkoinen määrä, niin palvelimessa tarvittavat **peruspalvelut** ovat seuraavat:

- **Alerter** (ei kuitenkaan pakollinen, jos ei haluta hälytyksiä)
- **Computer Browser** (selauspalvelu työasemille)
- **EventLog**
- **Messenger** (ei kuitenkaan pakollinen, jos ei haluta ilmoituksia)
- **Net Logon**
- **Remote Procedure Call (RPC) Locator**
- **Remote Procedure Call (RPC) Service**
- **Schedule** (ei pakollinen, jos ei ajasteta toimintoja**)**
- **Server**
- **Spooler** (ei kuitenkaan pakollinen)
- **TCP/IP NetBIOS Helper** (ei kuitenkaan pakollinen, jos ei käytetä TCP/IP-protokollaa)
- **Workstation**.

Tämän listan avulla voit tarvittaessa pysäyttää palvelimesta tarpeettomat palvelut. Palvelut toki riippuvat toisten palvelimein ja työasemien konfiguroinnista sekä käytettävistä protokollista, joten koko ympäristön tuntemus on ensiarvoisen tärkeätä hallittaessa NT:n palveluita.

NetLogon

Net Logon-palvelu huolehtii seuraavista:

- Käyttäjien verkkoonkirjautuminen (NT-työasemien toimialueelle kirjautuminen hoidetaan NT-palvelimen ja NT-työaseman oman Net Logon-palvelun avulla)

- Kirjauskomentojonojen välitys käyttäjän kirjautuessa (**NETLOGON**-jaon avulla)

- Käyttäjätietokannan päivittäminen toimialueen ohjauskoneiden välillä.

Windows NT -palvelimen NetLogon-palvelu synkronoi automaattisesti käyttäjätietokannat. Rekisterin asetusten mukaan PDC lähettää säädetyin

aikavälein ilmoituksia, joiden perusteella BDC:t lähettävät käyttäjätietokannan päivityspyyntöjä PDC:lle. Pyynnöt porrastetaan siten, etteivät BDC:t pyydä päivityksiä samanaikaisesti. Kun BDC pyytää päivitystä, se kertoo samalla PDC:lle viimeksi saamastaan päivityksestä, joten PDC on selvillä BDC:n päivitystarpeista. Jos BDC on ajantasalla, BDC:n Net Logon palvelu ei pyydä päivitystä.
PDC:n muutoslokiin tallennetaan muutokset käyttäjätietokannassa. Lokin koolle annetut asetukset määrittelevät, kauanko muutokset pidetään siinä. Oletus on viisi (**5**) minuuttia ja **2000** muutosta. Jos BDC ei pyydä sallituissa aikarajoissa päivitystä, koko käyttäjätietokanta kopioidaan BDC:lle:

- **Osittainen synkronointi** (*Partial synchronization*) on automaattinen, ajastettu toiminto, joka lähettää käyttäjätietokannan muutokset BDC:eille

- **Täydellinen synkronointi** (*Full synchronization*) lähettää koko käyttäjätietokannan BDC:lle. Tällainen tilanne tulee, kun muutoslokissa olevat tiedot on poistettu ennenkuin käyttäjätietokannan muutosten kopiointi tapahtui tai kun uusi BDC lisätään toimialueelle

Kun NT-työasema käynnistyy, se etsii ohjauskoneen omasta ja luotetuista toimialueista. Kun ohjauskone löytyy, sitä käytetään käyttäjän kirjautumispyynnön käsittelyyn.

Kun ohjauskone käynnistyy, se etsii ohjauskoneen luotetuista toimialueista. Omasta toimialueesta ei tarvitse etsiä ohjauskonetta, koska tietokannan kopio on jo NT-plavelimessa. Jokaista toimialuetta kutsutaan kolme kertaa viiden sekunnin välein. Jos vastaus ei tule tänä aikana,yritetään uudelleen 15 minuutin välein. Jos tällöin tulee kirjautumispyyntö, yhteyttä toiseen toimialueeseen yritetään kuitenkin välittömästi.

Suojattu kanava (*Secure Communication Channel*) on menetlmä, jossa Net Logon -palvelu tarkistaa tietokoneen tunnuksen (*Computer Account*) olemassaolon. Jos näin on, yhteys muodostetaan tietokoneiden välille tiettyjen käyttäjätunnusten avulla:

- **Työasematunnukset** (*Workstation trust accounts*), joiden avulla käyttäjä kirjautuu toimialueelle. Kun käyttäjä kirjautuu ensimmäisen kerran, ohjauskone palauttaa NT-työasemaan paikalliseen tietokantaan tiedot, joilla käyttäjän kirjautuminen

toimialueelle sallitaan *vaikka* ohjauskone ei vastaisikaan. Kyseessä on ns. *cached information* ja oletuksena tallennetaan **10 edellistä** kirjautumista

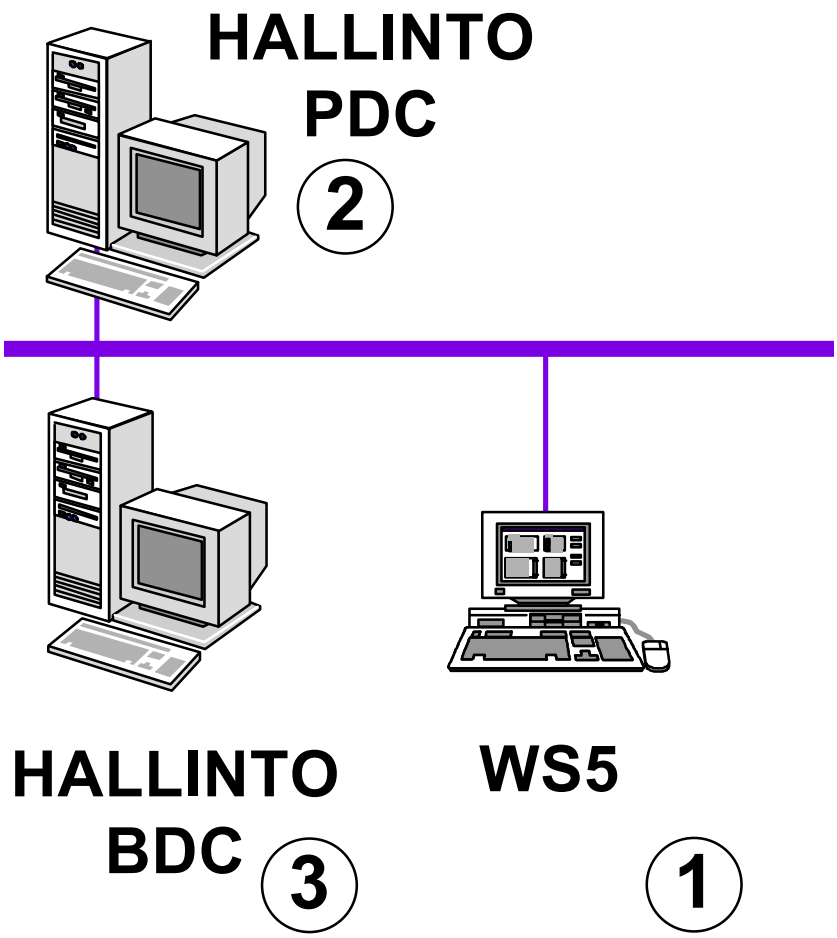
- **Palvelintunnukset** (*Server trust accounts*), joiden avulla ohjauskoneet päivittävät käyttäjätietokantaansa

- **Toimialuiden väliset luottosuhteet** (*Interdomain trust accounts*), joiden avulla käyttäjän kirjautuminen välitetään toiselle toimialueelle.

Käytännön esimerkki: pääkäyttäjä on juuri päivittänyt HALLINTO-toimialueen PDC-palvelimelle käyttäjän uuden salasanan.

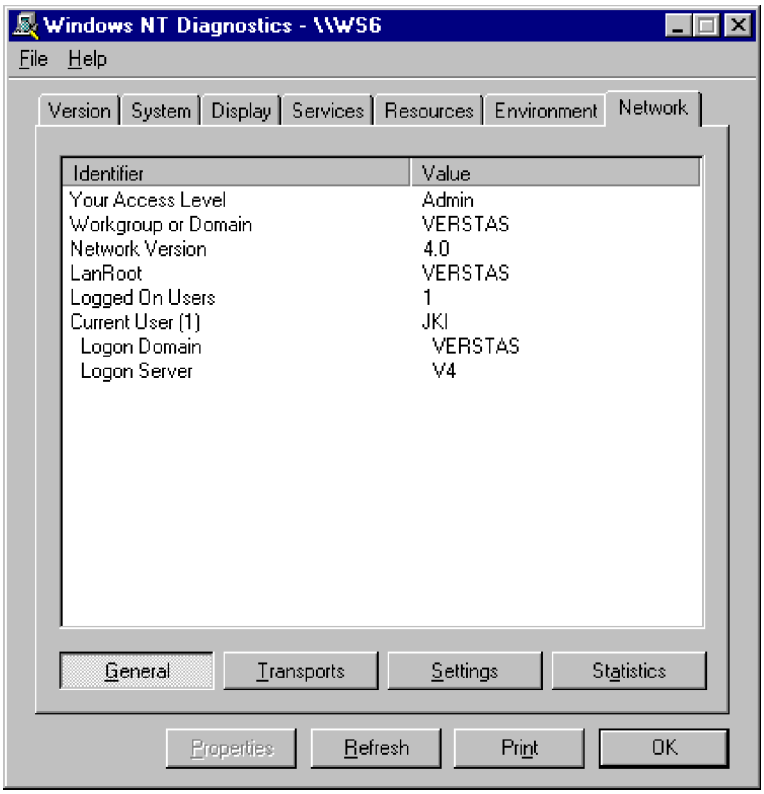
Käyttäjä kirjautuu HALLINTO-toimialueelle WS5-työasemastaan (**1**), eikä pääse kirjautumaan uudella salasanalla.

Syynä on todennäköisesti se, että vaikka salasanan päivitys on PDC:ssä (**2**), käyttäjätietokannan päivitys ei ole ehtinyt HALLINTO-toimialueen BDC-palvelimelle (**3**), joka käsitteli käyttäjän kirjautumispyynnön.



Ratkaisu on joko päivittää käyttäjätietokanta **Server Manager**-ohjelmalla tai odottaa muutama minuutti.

Kirjautuminen voidaan tarkistaa NT-työasemassa **Windows NT Diagnostics**-ohjelmalla. **Network**-välilehden **Logon Server** kertoo palvelimen, joka käsitteli käyttäjän verkkoonkirjautumisen. Koska **Windows NT Diagnostics**-ohjelma toimii myös verkon yli, pääkäyttäjä voi tarkistaa, mikä palvelin käsitteli käyttäjän verkkoonkirjautumisen.



Net Logon-asetuksia voidaan säätää rekisterissä palvelun asetuksista. Esimerkiksi laajassa verkossa käyttäjätietokannan päivitykseen liittyviä asetuksia voi tarvittaessa muuttaa. Keskeisiä asetuksia ovat seuraavat:

- **Pulse** määrittelee päivitysvälin, jonka aikana tehdyt SAM/LSA -muutokset kootaan yhteen ja annetun ajan jälkeen lähetetään BDC-palvelimille ilmoitus käyttäjätietokannan muuttumisesta. Ilmoitusta ei lähetetä BDC:lle joka on ajan tasalla. Jos asetusta ei anneta, NetLogon optimoi arvon PDC:n kuormituksen mukaan.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Netlogon\Parameters**
Nimi	**Pulse**
Tyyppi	**REG_DWORD**
Arvo	**60 - 172800 sekuntia (48 tuntia), oletus 300 (5 minuuttia)**

- **PulseConcurrency** määrittelee PDC:n samanaikaisesti BDC:eille lähettämien pulssien määrän. Arvon kasvatus lisää PDC:n kuormitusta ja arvon pienentäminen hidastaa käyttäjätietokantojen päivitysnopeutta.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Netlogon\Parameters**
Nimi	**PulseConcurrency**
Tyyppi	**REG_DWORD**
Arvo	**1 - 500 pulssia, oletus 20**

- **ReplicationGovernor** määrittelee sekä miten usein että miten paljon käyttäjätietokannan päivitystietoja kerrallaan päivitetään. Asetuksella 50 käytetään 64 kt puskuria (100% = 128 kt) ja vain 50% käyttäjätietokannan päivityspyynnöistä lähetetään. Jos arvo on liian pieni, käyttäjätietokannan päivitys ei koskaan valmistu ja arvolla 0 käyttäjätietokannan päivitys ei toimi. Asetus voidaan asettaa BDC-kohtaisesti riippuen sekä verkon kuormituksesta että vaikkapa kellonajasta. Apuna voi käyttää AT-komennolla ajastettua rekisterin päivitystä kahdesti päivässä.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Netlogon\Parameters**
Nimi	**ReplicationGovernor**
Tyyppi	**REG_DWORD**
Arvo	**0 -100 (prosenttia, oletus 100)**

- Viimeinen oleellinen asetus on **Update**. Jos se saa arvon **Yes**, käyttäjätietokanta päivitetään aina ohjauskoneen käynnistyessä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Netlogon\Parameters**
Nimi	**Update**
Tyyppi	**REG_SZ**
Arvo	**Yes tai No (oletus)**

Net Logon huolehtii myös toimialueiden välisten luottosuhteiden ylläpidosta. Koska toimialueita yhdistetään nykyisin myös ISDN-yhteyksin, seuraavat asetukset kannattaa huomioida.

- **ScavengeInterval**-parametri (tyyppi REG_DWORD) määrittelee, kuinka usein Netlogon suorittaa seuraavat puhtaanapito-operaatiot (arvot sekunteina):

  - Tarkistaa, onko ohjauskoneiden välisen suojatun kanavan (*secure channel*) salasana vaihdettava

  - Tarkistaa, onko turvallinen kanava ollut hiljaa huomattavan kauan

  - Domain Controller -palvelimilla lähettää mailslot-viestin kullekin luotetulle toimialueelle, jolta ei ole löytynyt Domain Controlleria

  - Primary Domain Controllerissa yrittää lisätä NetBIOS-nimen [1Bh], ellei sitä jo ole lisätty

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Netlogon\Parameters**
Nimi	**ScavengeInterval**
Tyyppi	**REG_DWORD**
Arvo	**Oletusarvo on 900 sekuntia (15 minuuttia). Minimiarvo on 60 sekuntia ja maksimi 172800 (kaksi vuorokautta)**

Yksikään yllä luetelluista operaatioista ei ole järjestelmän toiminnan kannalta kriittinen, eikä 15 minuutin oletusarvoa ole syytä muuttaa kuin erityisistä syistä. Esimerkiksi, jos Domain Controllerin ja luotetun palvelinalueen välissä on kallis ISDN-linkki, arvoa voi kasvattaa. Tällöin automaattisten yhteydenottojen määrä vähenee ja linjakustannukset pienenevät.

- **ExpectedDialupDelay** -parametri (tyyppi REG_DWORD) määrittelee ajan, joka reitittimeltä normaalisti kuluu yhteyden muodostamiseen, kun NT-palvelin haluaa lähettää viestin luotetulle toimialueelle. Tavallisesti Domain Controllerin tavoittamiseen kuluva aika on varsin lyhyt, esimerkiksi 15 sekuntia. Tätä parametria käyttämällä odotusaikaa voidaan kuitenkin kasvattaa. Parametrin muuttaminen vaikuttaa seuraaviin kahteen asiaan:

  - Kun järjestelmä havaitsee ohjauskoneen luotetulla palvelinalueella, Netlogon lähettää kolme mailslot-viestiä luotetulle palvelinalueelle. Viestien väli on **5 + ExpectedDialupDelay / 3** sekuntia. Synkroniset havainnot ohjauskoneista eivät vanhene aikana, joka on **kolme** kertaa tämän välin pituinen

  - **API-kutsu**, joka on lähetetty turvallista kanavaa pitkin havaitulle Domain Controllerille, vanhenee (45 + ExpectedDialupDelay) sekunnin kuluttua.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Netlogon\Parameters**
Nimi	**ExpectedDialupDelay**
Tyyppi	**REG_DWORD**
Arvo	**Oletusarvo on 0 sekuntia, maksimi 600 sekuntia**

Oletusarvo on nolla sekuntia ja maksimi 600 sekuntia (10 minuuttia). Tätä parametria tulee muuttaa vain, jos palvelimen ja luotetun toimialueen välissä on puhelinverkkoreititin. Jos arvo asetetaan liian suureksi, järjestelmältä saattaa mennä huomattavasti aikaa, ennen kuin se havaitsee luotetun palvelinalueen ohjauskoneen puuttumisen.

Computer Browser

Menetelmä, jolla Työryhmä-Windows-, Windows 95- ja Windows NT-koneet löytävät verkon resursseja, on nimeltään **selauspalvelu** (*Browser*).

Käyttäjän selatessa verkkoa (**Network Neighborhood**-ikkunassa, **File Managerissa** tai komentorivin **NET VIEW** -komennolla), hän saa listan verkon resursseista **selauspalvelimelta**. Tällainen keskitetty selausjärjestelmä vähentää verkon kuormitusta vähentämällä yleislähetysten (*broadcast datagrams*) määrää verkossa. Samalla työaseman (asiakkaan) prosessorikuormitus vähenee.

Selauspalvelun ongelma on se, että selauspalvelimen lista ei aina ole ajan tasalla. Listalla voi olla palvelimia/työasemia, jotka eivät ole enää verkossa tai jotka eivät ole vielä ehtineet ilmoittaa olemassaolostaan selauspalveluun.

Palvelimen / työaseman verkossaolon voit kuitenkin aina tarkistaa komentorivin **NET VIEW \\konenimi** -komennolla tai **File Managerissa** kirjoittamalla **Path**-kohtaan etsittävän palvelimen/työaseman nimen ja painamalla **OK**.

Laajassa reititinverkossa selauspalvelun toimintaan vaikuttavat seuraavat seikat:

- WINS-palvelu ja WINS-palvelimien konfigurointi
- LMHOSTS-tiedostot
- Protokollat (myös oletusprotokollat)
- Reitittimien konfigurointi
- Luottosuhteet
- Windows NT-palvelimien konfigurointi
- Windows NT- ja Windows 95-koneiden rekisterien asetukset
- Työryhmä-Windowsin SYSTEM.INI-asetukset
- Windows NT Service Packit
- Työryhmä-Windowsin päivitykset.

Kannattaa huomata, että kyseessä **ei** ole nimiselvitys, vaan nimenomaan verkon selauspalvelu.

Selauspalvelun komponentit

Selausjärjestelmä pitää luetteloa kaikista käytettävissä olevista toimialueista ja palvelimista ja se sisältää seuraavat komponentit:

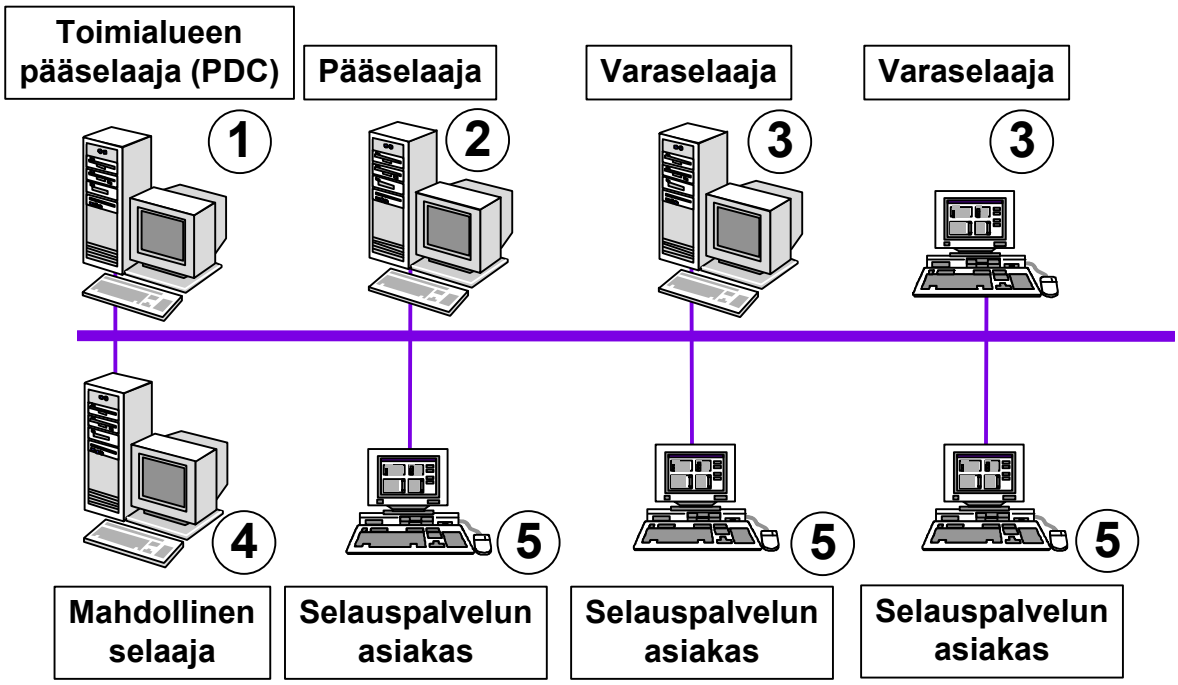
- **Toimialueen pääselaaja** (*Domain Master Browser*) (**1**) on aina toimialueen **ensisijainen ohjauskone** (*PDC, Primary Domain Controller*). Reitinverkossa se ylläpitää koko toimialueen selauslistaa

- **Pääselaaja** (Master Browser)(**2**) ylläpitää selauslistaa ja lähettää määräajoin kopion varaselaajille (Backup browser)

- **Varaselaajat** (Backup Browsers) saavat selauslistan pääselaajalta ja lähettävät sen asiakkaille

- **Mahdollinen selaaja** (Potential Browser) voi tarvittaessa ryhtyä (vaalin tuloksena) pääselaajaksi tai voi toimia varaselaajana, jos pääselaaja niin määrää

- **Asiakkaat** (Clients) saavat varaselaajilta selauslistan työasemiinsa.



Selauslistan koko on rajoitettu 64 kilotavuun. Tällöin listassa voi yhtä toimialuetta tai työryhmää kohti olla 2000-3000 mikroa.
Montako tietokonetta sitten osallistuu itse selauspalveluun?
Selausjärjestelmän toimintaan vaikuttaa LAN:in topologia ja eri tyyppisten mikrojen lukumäärä:

- Reititinverkossa jokaisessa aliverkossa on **pääselaaja** (*Master Browser*) ja LAN:in tai WAN:in piirissä on **yksi toimialueen pääselaaja** (*Domain Master Browser*)

- NT-toimialueella **jokainen ohjauskone** on selauspalvelin. Yksi palvelimista on **pääselaaja** ja toiset ovat **varaselaajia**

- Jos toimialueella on vähemmän kuin kolme (3) ohjauskonetta, Windows 95- tai Työryhmä-Windows-mikro voi ryhtyä toimimaan varapalvelimena

- NT-työryhmässä, jossa on Windows NT -työasemia, on aina yksi pääselaaja. Jos työryhmässä on kaksi työasemaa, toinen on varapalvelin. Jokaista 32:a Windows NT työasemaa kohti työryhmässä on aina yksi uusi varaselaaja

- Jos NT-toimialueella on enemmän kuin yksi NT-palvelin, yksikään NT-työasema ei ryhdy varaselaajaksi.

Selauspalvelimien lukumäärä päätellään seuraavan taulukon mukaan:

Tietokoneiden lukumäärä	Varaselaajien lukumäärä	Pääselaajien lukumäärä
1	0	1
2 - 31	1	1
32 - 63	2	1
64 -	Jokaista uutta 32 tietokonetta kohti yksi uusi varaselaaja	1

Selauspalvelun toiminta

Selauspalvelu toimii jokaisessa **työryhmässä** ja **toimialueessa**. **Asiakas** saa selauslistan seuraavasti:

1) Se lähettää API-kutsun pää- tai varaselaajalle (NetServerEnum2 API-kutsu, joka on LAN Manager-yhteensopiva)

2) Jos kyseessä on ensimmäinen kerta, kun selauslistaa pyydetään, asiakas lähettää **QueryBrowserServers**-tietosähkeen, johon **pääselaaja** vastaa palauttamalla listan kyseisen **työryhmän** tai **toimialueen varaselaajista**

3) Asiakas valitsee kolme nimeä listasta ja tallentaa nimet. Jatkossa lähetettävät **NetServerEnum**-kutsut lähetetään **satunnaisesti** jollekin näistä kolmesta varaselaajasta.

Jos asiakas ei löydä pääselaajaa kolmen yrityksen jälkeen, asiakas lähettää verkkoon **ForceElection**-yleissanoman (*broadcast*). Tällöin käynnistyy **vaalit**.

Jokaisella protokollalla on oma selauspalvelunsa. Esimerkiksi **nbf** viittaa NetBEUI-protokollaan ja **Nbt** TCP/IP-protokollaan. Niinpä työaseman käyttämällä oletusprotokollalla voi olla merkitystä siihen, mitä työasema verkosta näkee, varsinkin jos NT-palvelimissa on vaihteleva valikoima protokollia.

Jos käytössä on työryhmiä (NT-työasema asennettu työryhmätasolle, tai Windows 95- tai Työryhmä-Windows määritelty omaan työryhmäänsä), niin jokaisessa työryhmässä on oma pääselaajansa. Työryhmissäkin noudatetaan edellistä taulukkoa selauspalvelimien lukumäärästä. Ongelmaksi voi tulla työryhmien selauspalvelun toiminta, koska pää- ja varaselaajat ovat työasemia. Käyttäjän sulkiessa työasemansa työryhmän selauspalvelu järjestellään uudelleen, ja selauslista voi olla varsin sekaisin jonkin aikaa. Ratkaisu on määritellä nämä työasemat mukaan johonkin toimialueeseen, jossa selauspalvelua ylläpitävät Windows NT-palvelimet.

Kannattaa huomata, että toimialueella siitäkin huolimatta saattaa sopivassa konfiguraatiossa Windows 95- tai Työryhmä-Windows-työasemakin ryhtyä varaselaajaksi (tai peräti pääselaajaksi). Ratkaisu on kytkeä selauspalveluun osallistuminen pois näissä tietokoneissa myöhemmin neuvotulla tavalla.

Selauspalvelun synkronointi

Selauspalvelun synkronointi on toteutettu seuraavsti:

- Kun mikro ryhtyy pääselaajaksi, se lähettää ilmoituksen toimialueesta **DomainAnnouncement**-tietosähkeellä kerran minuutissa viiden minuutin ajan; tämän jälkeen kerran 15:ssä minuutissa. Tällöin muiden toimialueiden pääselaajat lisäävät toimialueen nimen omaan selauslistaansa. Toimialue poistetaan selauslistasta, jos se ei ole ilmoittanut itsestään **45:een minuuttiin** (3 * 15 minuuttia).

- Jos toimialue ulottuu useaan aliverkkoon, aliverkon pääselaajat synkronoivat itsensä **toimialueen pääselaajan** (*Domain Master Browser*) kanssa. Jos pääselaaja ei ole ohjauskone (PDC), pääselaaja synkronoi itsensä PDC:n kanssa. Samalla toimialueen pääselaaja lisää ylläpitämälleen selauslistalle aliverkon pääselaajan selauslistan. Tämä toistuu 15:n minuutin välein. Myös pääselaaja ja varaselaajat synkronoivat listansa kerran 15:ssa minuutissa.

  Kun mikro käynnistyy, se ilmoittaa itsestään toimialueen tai työryhmän pääselaajalle kerran minuutissa. Aikaväliä kasvatetaan 12:een minuuttiin

- Jos haluat lähettää selailutietoja myös LAN Manager 2.x-version asiakkaille, yhteensopivuus saadaan aikaan **Ohjauspaneelissa Network**-kuvakkeella valitsemalla **Server**-palvelun asetuksissa **Make Browser Broadcasts to LM 2.x Client**. Työasemassa et voi muuttaa näitä asetuksia

- Kun **varaselaaja** ajetaan alas, se ilmoittaa pääselaajalle poistumisestaan, ja pääselaaja poistaa tietokoneen selauslistalta

- Kun **pääselaaja** ajetaan alas, se lähettää **ForceElection**-tietosähkeen, mikä käynnistää vaalit

- Jos asiakas ei löydä pääselaajaa kolmen yrityksen jälkeen, asiakas lähettää verkkoon **ForceElection**-yleissanoman, mikä käynnistää vaalit

- Jos toimialueen pääselaaja kaatuu ja se on PDC, voit nostaa BDC:n **Server Managerilla** PDC:ksi

- Jos pääselaaja kaatuu, varaselaaja lähettää **ForceElection**-tietosähkeen 15 minuutin sisällä, mikä käynnistää vaalit. Tällä välin kyseinen työryhmä tai toimialue ei ehkä ole selattavissa muissa työryhmissä ja toimialueissa

- Jos mikro ei ilmoita itsestään **36**:een minuuttiin (**3** * **12** minuuttia), se poistetaan listasta

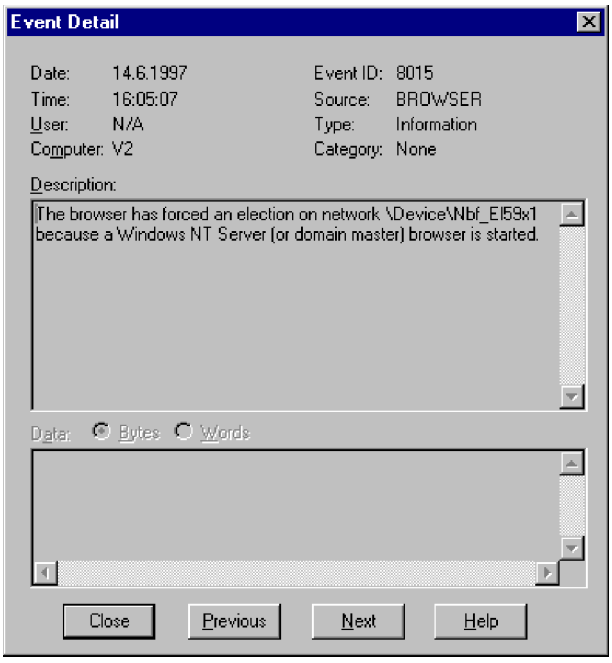
- Saattaa kestää kuitenkin peräti **51** minuuttia ennen kuin tietokone on poistettu selauslistalta, koska pääselaaja synkronoi varaselaajien listat oletuksena **15** minuutin välein.

Vaalit

Pääselaajasta voidaan tarvittaessa järjestää **vaalit** (*Election*). Tämä tarkoittaa algoritmia, joka ratkaisee, mikä palvelin ryhtyy suorittamaan pääselaajan tehtäviä.

Vaalit järjestetään kun:

- Tietokone ei löydä paikallista pääselaajaa
- Kun **suositeltava pääselaaja** (*Preferred Master Browser*) käynnistyy
- Kun ohjauskone käynnistyy.



Vaalin lopputuloksen ratkaisee seuraavat tekijät:

- Jos paikallisen mikron valmiudet tai ehdot ryhtyä toimimaan pääselaajana ovat suuremmat kuin vaalin käynnistäjän, paikallinen mikro voittaa. Esimerkiksi Windows NT -mikro voittaa Työryhmä-Windows-mikron
- Jos mikro on ollut pidempään verkossa kuin vaalin käynnistäjä, se voittaa

- Palvelin, jonka nimi on aikaisemmin aakkosissa, voittaa - esimerkiksi palvelin nimeltä **ATK1** voittaa palvelimen **VERSTAS1**

Suositeltava pääselaaja (*Preferred Master Browser*) on palvelin, joka on konfiguroitu voittamaan vaalit ja tulemaan seuraavaksi pääselaajaksi. TCP/IP-verkossa **ilman WINS:iä** on syytä määritellä tällaiset palvelimet hoitamaan toimialueen selailun ja NetBIOS-nimiselvityksen.

Seuraavan listan mukaisesti **käyttöjärjestelmä** vaikuttaa vaalin lopputulokseen:

- Windows NT Server 4.0 (PDC)
- Windows NT Server 3.51 (PDC)
- Windows NT Server 3.5 (PDC)
- Windows NT Server 3.1 (PDC)
- Windows NT Workstation 4.0
- Windows NT Workstation 3.51
- Windows NT Workstation 3.5
- Windows NT Workstation 3.1
- Windows 95
- Työryhmä-Windows (Windows For Workgroups) 3.11

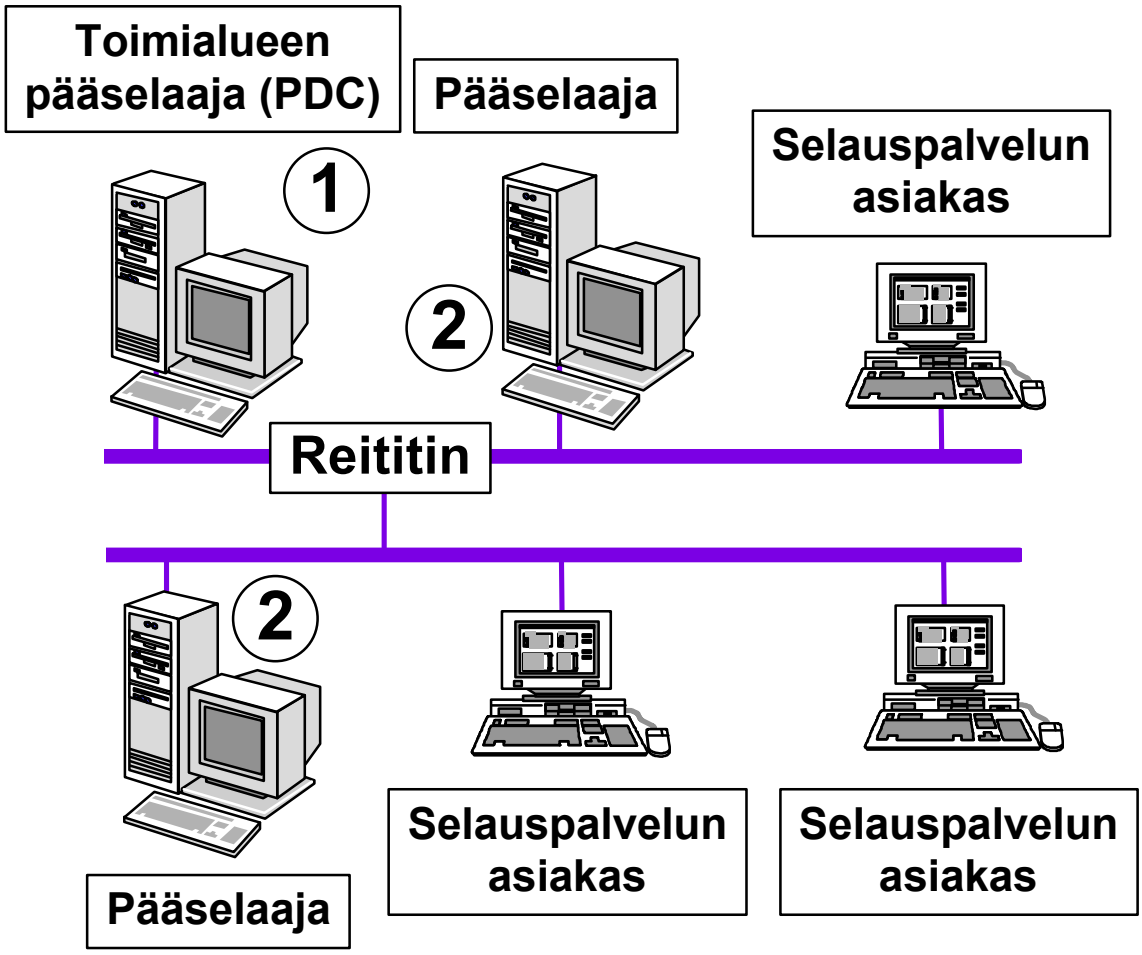
Muut vaikuttavat määritykset:

- Preferred Master (Windows NT)
- Master käynnistetty
- *Maintain-ServerList = Yes*
- Backup Browser käynnistetty

Selauspalvelu reititinverkossa

Toimialueen pääselaaja (*Domain Master Browser*) (**1**) on aina toimialueen **ensisijainen ohjauskone** (*PDC, Primary Domain Controller*). Reitinverkossa se ylläpitää koko toimialueen selauslistaa.

Jokaisessa segmentissä on oma pääselaajansa (**2**). Se voi olla Windows NT-palvelin, Windows NT-työasema, Windows 95- tai Työryhmä-Windows (Windows For Workgroups) -työasema.



Jos toimialue ulottuu useiden verkkosegmenttien alueelle, pääselaajat lähettävät osoitetun **MasterBrowserAnnouncement**-tietosähkeen toimialueen pääselaajalle. Se kertoo, että kyseinen pääselaaja on yksi toimialueen pääselaajista ja että toimialueen pääselaajan on lisättävä kyseisen pääselaajan selauslista toimialueen selauslistalle.

Toimialueen pääselaaja pyytää tämän jälkeen pääselaajan selauslistaa ja lisää sen toimialueen selauslistalle. Jatkossa tämä tehdään 15 minuutin välein.

Työryhmät **eivät** voi sijaita selauspalvelun kannalta eri verkkosegmenteissä. Niitä käsitellään tällöin kahtena **eri mutta saman nimisenä** työryhmänä.

Koska selauspalvelu perustuu yleissanomiin ja reititinverkoissa ne on tyypillisesti estetty, tästä seuraa ainakin kaksi selvitettävää tilannetta:

- Kuinka selaajat ylipäätään toimivat
- Kuinka asiakkaat voivat selata reititinverkon työryhmiä/toimialueita.

Selauspalvelu reititinverkoissa voidaan toteuttaa seuraavilla menetelmillä:

- **LMHOSTS**-tiedostoilla. Selauspalvelimissa tulee olla toimialueen pääselaajan rivillä **#DOM**-avainsana (esimerkiksi **130.9.63.5 V1 #PRE #DOM:VERSTAS**). Jos LMHOSTS-tiedostoa käytetään, siinä tulee olla määriteltyinä kaikki eri verkkosegmentissä sijaitsevat tietokoneet. Työasemat, jotka eivät ole WINS-asiakkaita, tarvitsevat kuitenkin LMHOSTS-tiedoston
- Avaamalla **UDP**-portti **137** (NetBT Name Service) reitittimissä. Tällöin selauspalvelun kannalta kyseessä on yksi verkko
- Yksinkertaisin menetelmä on WINS-palvelin (ks. Luku **8**). Se tukee paitsi nimiselvitystä, myös selauspalvelua. Työasemat, jotka eivät ole WINS-asiakkaita, tarvitsevat silti LMHOSTS-tiedoston.

Selauspalvelun NetBIOS-nimi on **--__MSBROWSE__- <01h>**.

Selauspalvelun konfigurointi

Selauspalvelun asetukset löytyvät rekisteristä.

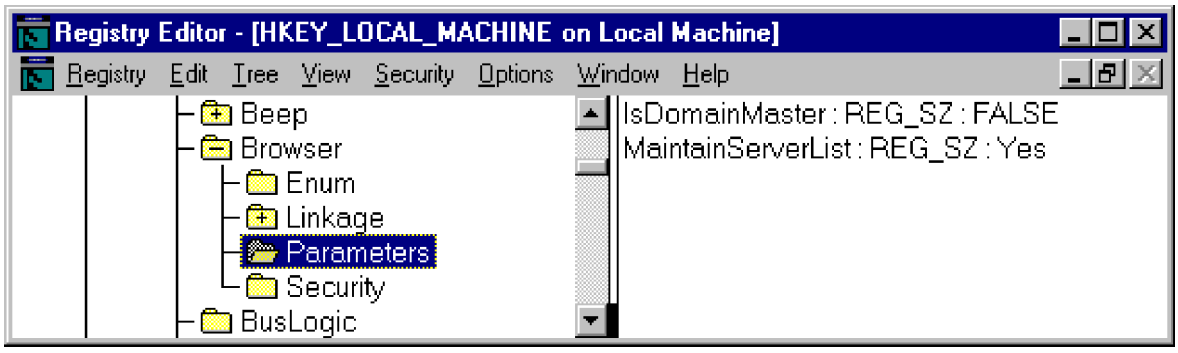
Selaajien asetuksia ovat mm. seuraavat:

- **BackupPeriodicity** määrittää miten usein varaselaaja ilmoittaa itsestään pääselaajalle. Ei vaikuta reititinverkossa, koska kyseessä on aina paikallinen aliverkko. Asetuksen muuttaminen vaatii uudelleenkäynnistyksen

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Browser\Parameters**
Nimi	**BackupPeriodicity**
Tyyppi	**REG_DWORD**
Arvo	**720 (oletus), 300 – 4294967**

- **MasterPeriodicity** määrittelee miten usein pääselaaja ilmoittaa itsestään toimialueen pääselaajalle. Anna asetus kaikissa mahdollisissa pääselaajissa. Jos annat asetuksen toimialueen pääselaajassa, se määrittää, miten usein toimialueen pääselaaja pyytää selauslistaa WINS:ista. Jos arvo on liian pieni, reititinverkon liikenne saattaa lisääntyä.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Browser\Parameters**
Nimi	**MasterPeriodicity**
Tyyppi	**REG_DWORD**
Arvo	**720 (oletus), 300 – 4294967**



Selaajan asetukset:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Browser\Parameters**
Nimi	**MaintainServerList**
Tyyppi	**REG_SZ**
Arvo	**No - ei tule selaajaksi** **Yes - tulee selaajaksi. Käynnistyksen yhteydessä palvelin yrittää saada yhteyden pääselaajaan. Jos se ei onnistu, se käynnistää vaalit ja voi tulla pääselaajaksi. Tämä on oletus NT-palvelimissa** **Auto - palvelin on mahdollinen selaaja. Selaajaksi tulemi-nen riippuu olemassaolevista selaajista; tämä on oletus NT -työasemissa**

Asetuksilla **Yes** tai **Auto** selauspalvelu käynnistyy aina mikron käynnisty-essä.

Myös **suositeltava pääselaaja** (*Preferred Master Browser*) on asetettu rekisterissä.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Browser\Parameters**
Nimi	**IsDomainMasterBrowser**
Tyyppi	**REG_SZ**
Arvo	**No - ei tule selaajaksi** **Yes - asetetaan kyseinen NT-mikro suositeltavaksi pääselaajaksi (*Preferred Master Browser*). Tällöin sen käynnistyessä suoritetaan aina vaalit**

Työryhmä-Windows (Windows for Workgroups)-työasemissa estetään osallistuminen selauspalveluun seuraavalla asetuksella:

Tiedosto	**SYSTEM.INI**
Sektio	**[Network]**
Nimi	**MaintainServerList**
Arvo	**No - ei tule selaajaksi** **Yes - voi osallistua selauspalveluun (oletus)**

Windows 95-työasemissa estetään osallistuminen selauspalveluun Ohjauspaneelin **Verkon** (Network) valitsemalla palvelun **Tiedostojen ja kirjoittimien jakaminen Microsoft-verkoissa** (File and printer sharing for Microsoft Networks) **Browse Master**-asetukselle **No**. Vaihtoehdolla **Yes** osallistutaan aina selauspalveluun ja vaihtoehdolla **Auto** asetetaan **mahdollinen selaaja**.

Piilotettu tietokone

Jos **piilotat** NT-työaseman tai -palvelimen verkosta komennolla **NET CONFIG SERVER /HIDDEN:YES** se estää kyseistä mikroa ilmoittamasta olemassaolostaan selauspalvelulle. Sama voidaan asettaa rekisterin avulla:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\LanmanServer\Parameters**
Nimi	**Hidden**
Tyyppi	**REG_DWORD**
Arvo	**0 (oletus, ei piilotettu), 1 (piilotettu)**

Voit kuitenkin edelleenkin tarkistaa e.m. tietokoneen verkossaolon **Tiedostonhallinnassa** (File Manager) kirjoittamalla **Polku** (Path)-kohtaan palvelimen tai työaseman nimen ja painamalla **OK**. Saman voit tehdä komentorivin **NET VIEW \\konenimi** -komennolla.

Jaetut resurssit saat tällaisesta "piilotetusta" mikrosta käyttöösi kirjoittamalla **Tiedostonhallinnassa** (File Manager) **Polku** (Path)-kohtaan resurssin UNC-nimen, esimerkiksi **\\konenimi\resurssi** ja painamalla **OK** tai vastaavasti komentorivin **NET USE x: \\konenimi\resurssi** -komennolla.

Palvelun toiminnan voit tarkistaa **Ohjauspaneelissa** (Control Panel) **Palvelut** (Services-kuvakkeella. Tarkista, että **Tietokoneiden selaus** (Computer Browser) on käynnistetty.

Browser Monitor

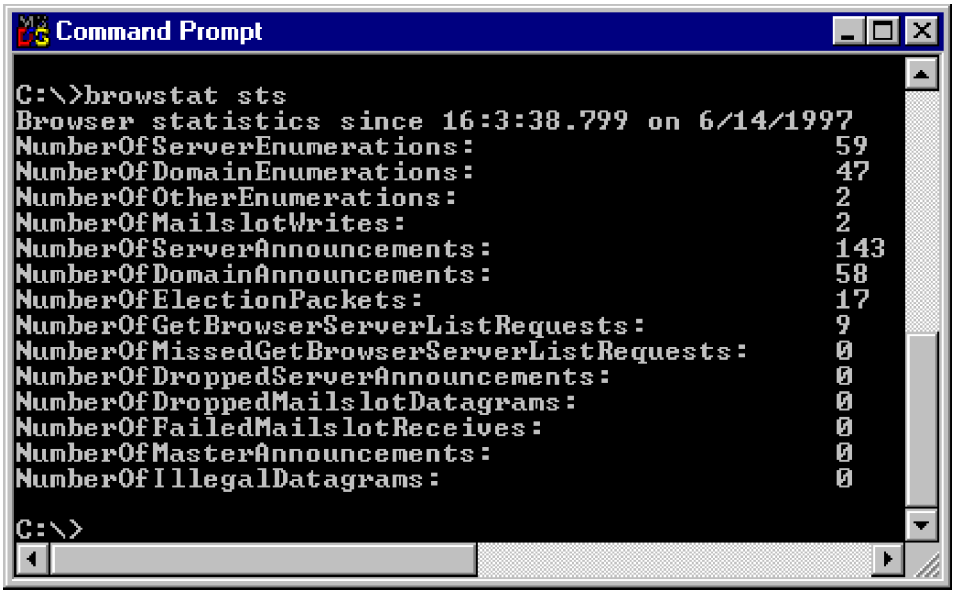
Selauksen seurantaa voidaan tehdä esimerkiksi Resource Kitin **Browser Monitor** -apuohjelmalla.

Koska selauspalvelu toimii kaikilla protokollilla samanaikaisesti, niin saatat törmätä seuraaviin protokollien lyhenteisiin: **Nbf** (**NetBIOS Frame**) liittyy **NetBEUI**:in, **NetBT** (**NetBIOS over TCP/IP**) liittyy TCP/IP:hen ja **NwlnkNb** (**NetWare Link NetBIOS**) liittyy **SPX/IPX**:ään.

Domain | Add Domain -valinnalla voit valita seurattavat toimialueet. Kaksoisnapauttamalla valitun palvelimen päälle näet lisätietoja.

Browstat

BROWSTAT.EXE on Resource Kitin apuohjelma, jolla voidaan tehdä moniakin selauspalvelun ylläpitotoimia.



Valitsimet ovat:

ELECT - käynnistä vaalit

GETBLIST - varaselaajien lista
GETMASTER - pääselaajan nimi
GETPDC - PDC:n nimi
LISTWFW - Työryhmä-Windows-koneet, jotka toimivat selaajina
STATS - selaajan status
STATUS - toimialueen status
TICKLE - pysäytä pääselaaja
VIEW - NetServerEnum

Aikakatkaisu

Aikakatkaisu (*Idle Session Time*) määrittelee, milloin ei-aktiivisen käyttäjän istunto katkaistaan.

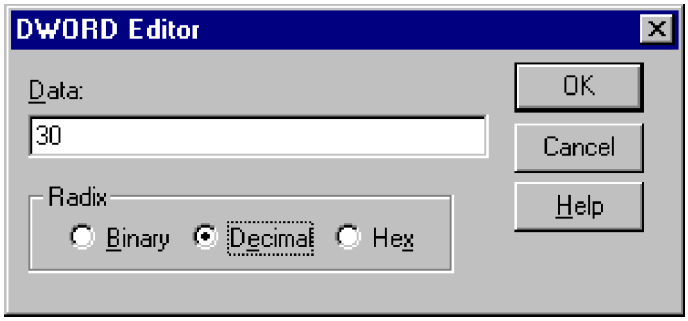
Voit asettaa järjestelmän katkaisemaan automaattisesti käyttäjien istunnot, jotka ovat olleet käyttämättä 60 minuutin ajan komentorivin komennolla:

NET CONFIG SERVER /AUTODISCONNECT:60

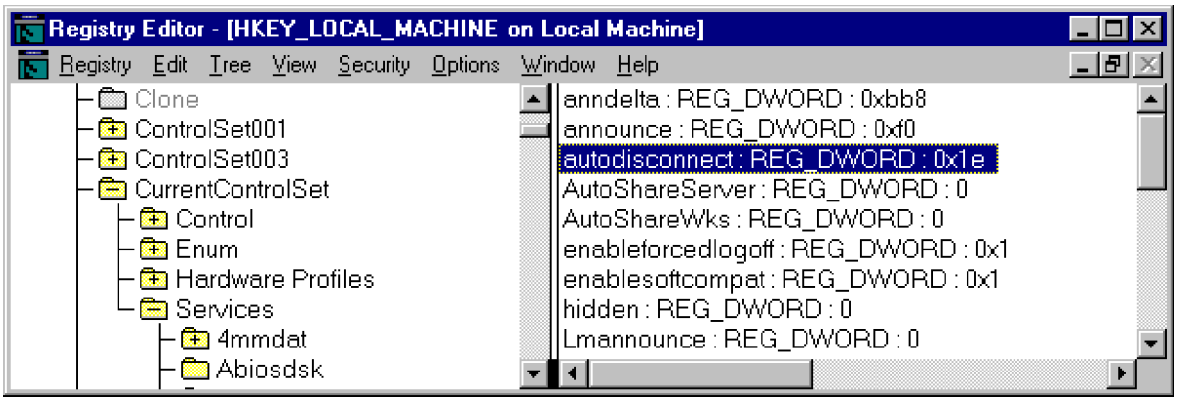
Asetus on rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\LanmanServer\Parameters**
Nimi	**AutoDisconnect**
Tyyppi	**REG_DWORD**
Arvo	**Aika minuutteina; oletus on 15**

Voit antaa asetuksen joko binaari-, desimaali- tai heksadesimaalilukuna:



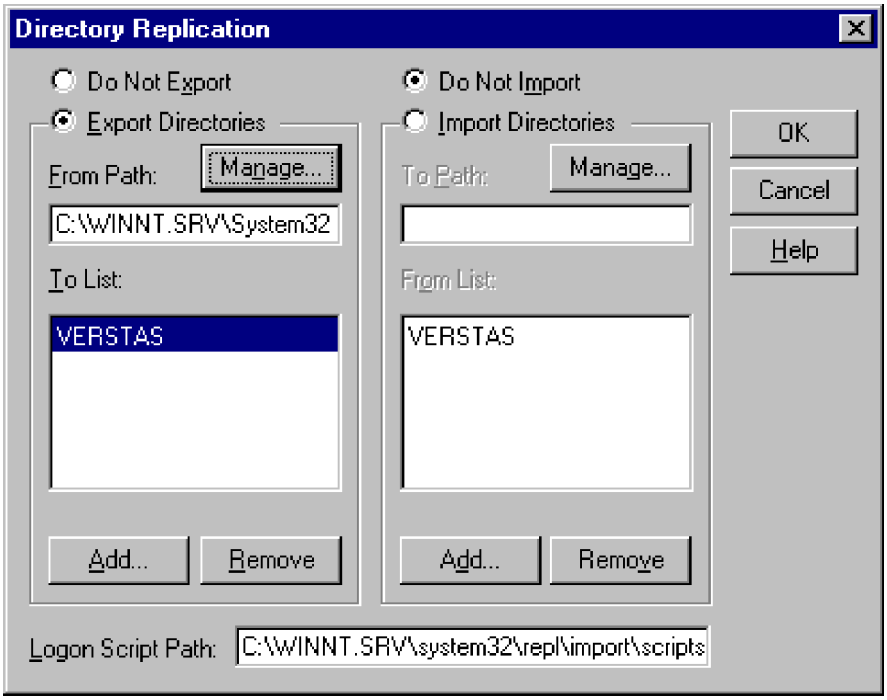
Esimerkiksi 30 minuuttia on **1e**:



Directory Replication

Monistuspalvelun (Directory Replication) avulla voidaan kopioida tiedostoja NT-palvelimista NT-palvelimiin tai NT-työasemiin.

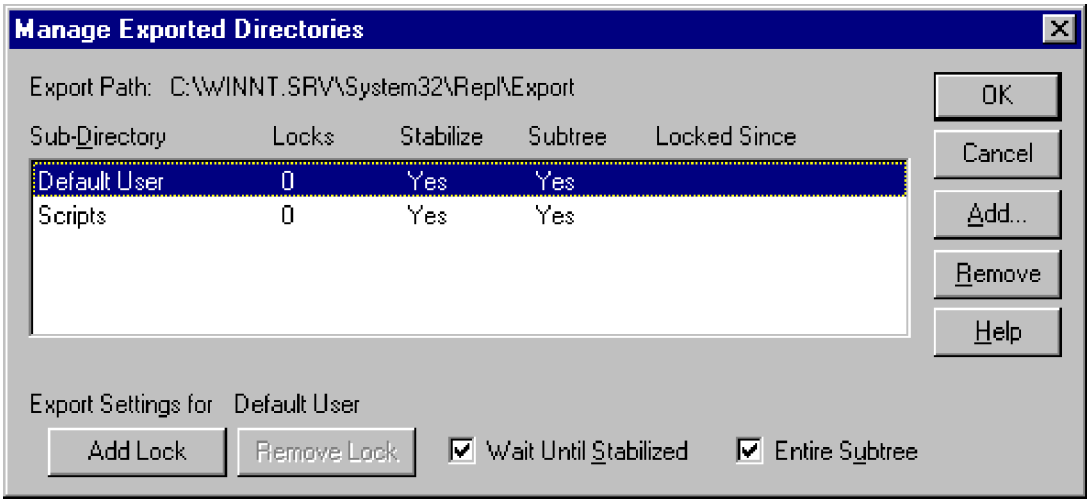
Palvelun konfigurointi sekä NT-palvelimissa että NT-työasemissa on käsitelty luvussa **3**.



Monistuksen kohteena olevat tiedostot ovat tyypillisesti käyttäjien kirjauskomentojonot eli *Logon scriptit*. Kyseessä on komentojono, joka suoritetaan automaattisesti käyttäjän kirjautuessa toimialueelle. Se voi olla komentojono (.BAT- tai .CMD) tai ohjelmatiedosto (.EXE). Kun palvelin tarkistaa, että käyttäjän sisäänkirjauspyyntö on oikea ja että

käyttäjälle on määritetty kirjauskomento, se paikantaa kirjauskomennon paikallisen hakemistopolun ja **User Manager for Domains**illa määritetyn tiedostonimen sekä haluttaessa sen suhteellisen polun (esimerkiksi **ADMINS\PCTUKI.BAT**).

Toimialueen kunkin kirjauskomentosarjan alkuperäiset kopiot kannattaa tallentaa vain yhteen Windows NT -palvelimeen (esimerkiksi toimialueen **Primary Domain Controller**) monistettavaan **vientihakemistoon**, josta ne monistetaan toimialueen muille palvelimille.



Tuotujen kirjauskomentojen hakemistopolku on sen jälkeen määritettävä **Directory Replication**-valintaikkunan **Logon Script Path**-ruutuun kussakin Windows NT-palvelimessa erikseen. Windows NT-työasemissa ei voi vaihtaa kirjauskomennon oletushakemistoa, joka on yleensä **C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS**. Eri asia on, onko palvelimissakaan syytä muuttaa kirjauskomennon oletushakemistoa.

Riippuen siitä, miten kirjauskomentosarjat halutaan tallentaa PDC:lle, joudutaan joko kopioimaan tiedostot kahteen paikkaan tai muuttamaan PDC:llä kirjauskomentosarjojen sijaintiasetusta.

Kirjauskomentosarjan asetusten määrittäminen palvelimelle tehdään määrittämällä **Logon Script Path**-ruutuun paikallinen hakemistopolku, oletuksena **C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS**. Hakemistopolku on pakollinen eikä ruutua ei voi jättää tyhjäksi. PDC:ssä tähän voi vaihtaa vientihakemiston **C:\WINNT\SYSTEM32\REPL\EXPORT**.

Toinen tapa kopioida hakemistoja palvelimelta toiselle on Resource Kitin **ROBOCOPY**-ohjelma.

Monistuspalvelun (Directory Replication) asetukset ovat rekisterissä seuraavasti:

- rekisterin **winreg**-avain määrittelee rekisterin etäkäyttöoikeudet. Windows NT-työasemissa tätä asetusta ei ole, ja Windows NT-palvelimissa oikeus on vain **Administrators**-ryhmän jäsenillä. Myös monistuspalvelun käyttäjätunnukselle on annettava lukuoikeus.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentcontrolSet\Control\SecurePipeServers\winreg**
Oikeus	**Administrator: Full Control, Replicator: Read**

- rekisterin Replicator-asetukset määrittelevät monistusmenettelyn. Asetusta **Interval** voi haluttaessa pienentää:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Replicator\Parameters**
Nimi	**Interval**
Tyyppi	**REG_DWORD**
Arvo	**1 - 60 minuuttia, oletus 5 minuuttia**

- asetus **GuardTime** määrittelee hakemiston sisällön vakiintumisen. Asetusta voi ehkä tarvittaessa kasvattaa:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Replicator\Parameters**
Nimi	**GuardTime**
Tyyppi	**REG_DWORD**
Arvo	**0 - puolet Interval-ajasta minuutteina, oletus 2 minuuttia**

Server Manager

NT-työaseman mukana ei tule **Server Manager**-ohjelmaa, mutta Windows 95- ja Windows NT 4.0 -työasemaversiot tulevat Windows NT 4.0 -palvelimen CD-ROM:in mukana, josta ne voi asentaa työasemaan.
Server Managerin avulla voit hallita toimialueita ja NT- tai LAN Manager -palvelimia ja NT-työasemia:

- Voit valita hallittavan toimialueen, työryhmän tai palvelimen/työaseman. Tämän jälkeen voit tarkastella palvelimeen/työasemaan yhteydessä olevien käyttäjien luetteloa, jaettuja ja avoimia resursseja.

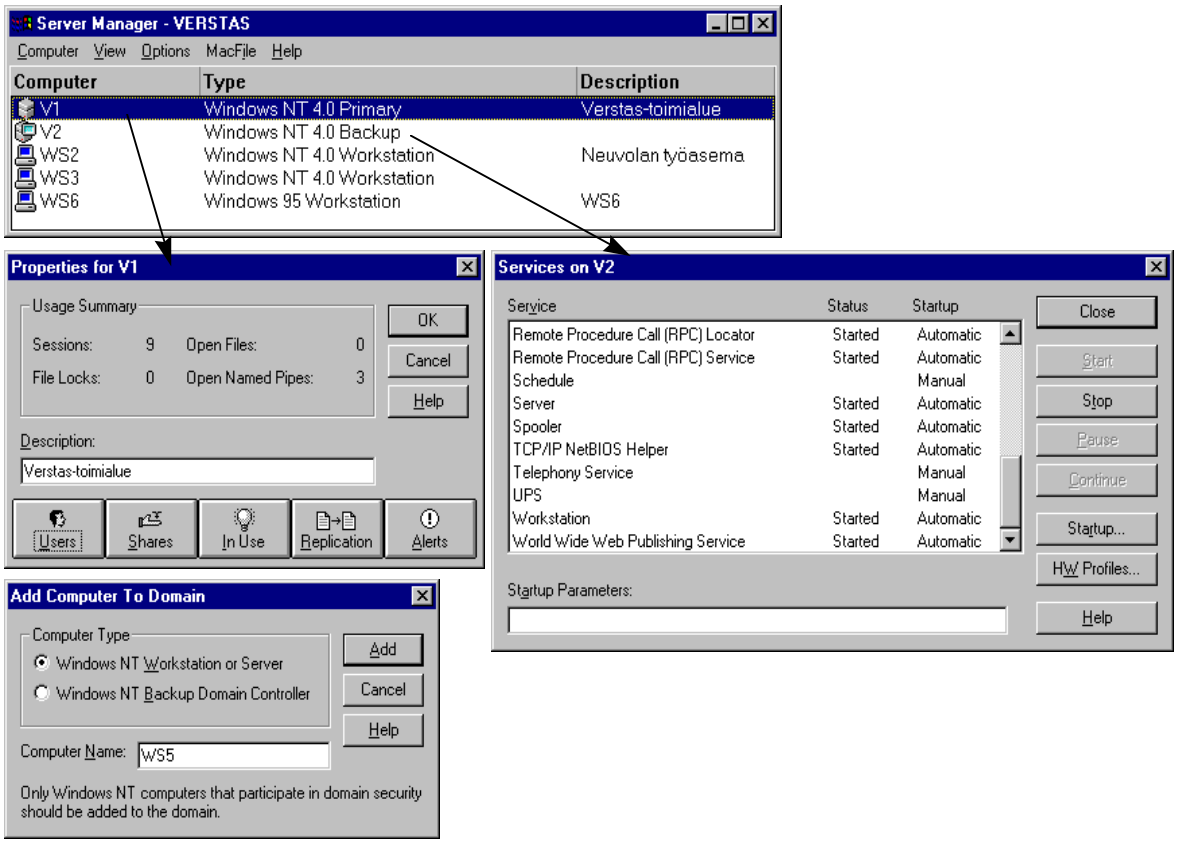
- Voit hallita hakemistojen monistamista (*replikointi*) ja valvontahälytysten (*alerts*) vastaanottajien luetteloa, palveluita ja jaettuja hakemistoja sekä lähettää viestejä palvelimeen/työasemaan yhteydessä oleville käyttäjille.

- Voit myös tehdä toimialueen hallintatoimia, kuten muuttaa palvelimen roolin toimialueen **pääohjauskoneeksi** (*Primary Domain Controller*, PDC), **tahdistaa** muut palvelimet toimialueen PDC:n käyttäjätietokannan kanssa sekä lisätä/poistaa yksittäisiä työasemia/palvelimia toimialueelle

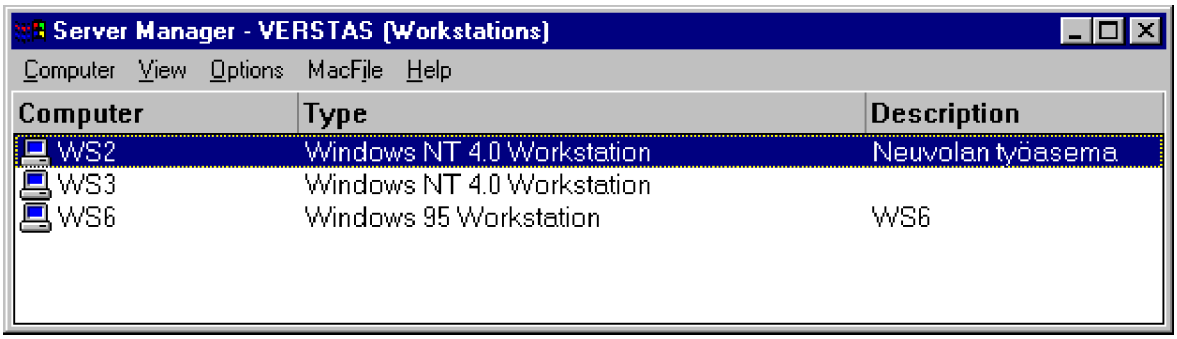
- Server Managerilla voi hallita paikallisen verkon tai etäyhteyden kautta toisen verkon NT-koneita etäyhteyden kautta verkkoon liittyneitä NT-koneita!

- Jotta voisit hallita toimialuetta ja sen palvelimia sinun on oltava kirjautuneena verkkoon toimialueen **Administrators**-, **Domain Admins**- tai **Server Operators**-ryhmän jäsenenä. Myös **Account Operators**-ryhmän jäsenet voivat käyttää Server Manageria, mutta he voivat vain lisätä NT-koneita toimialueelle

- Jotta voisit hallita NT-työasemaa sinun on oltava kirjautuneena kyseisen NT-työaseman **Järjestelmänvalvojat** (Administrators)- tai **Tehokäyttäjät** (Power Users)-ryhmän jäsenenä. Jos NT-työasema on lisätty toimialueelle, niin työaseman **Järjestelmänvalvojat** (Administrators)-ryhmään kuuluu oletuksena mukaan **Domain Admins**.



Oletuksena luettelossa näkyvät sekä palvelimet että työasemat. Voit halutessasi suodattaa luettelon ja näyttää vain toiset valinnalla **View** | **Servers** - tällöin otsikkorivillä lukee **(Servers)** ja **View**-valikossa on a.o. kohdassa valintamerkki. Vastaavalla tavalla voit tuoda vain työasemat **View** | **Workstations** tai kaikki **View** | **All** näyttöön.



Vain toimialueeseen kuuluvat työasemat/palvelimet näytetään, kun valitset **View** | **Show Domain Members Only**. Voit päivittää näytön valitsemalla **View** | **Refresh** tai painamalla **F5**.

Options-valikosta löytyvät valinnat asetusten tallentamiseen lopetettaessa **Save Settings on Exit**, käytetty fontti **Fonts** ja hidas yhteys **Low Speed Connection**, jota voit käyttää, kun kohteeseen on suhteellisen hidas tiedonsiirtoyhteys esimerkiksi RAS:in kautta. Vaihtoehto estää **Server Manager**-ikkunan automaattisen päivityksen. Päivitys voi kestää kauan, jos yhteys etäjärjestelmään on hidas; näyttö päivittyy automaattisesti eräiden toimintojen jälkeen.

Low Speed Connection -vaihtoehdon voi valita kahdella eri tavalla.

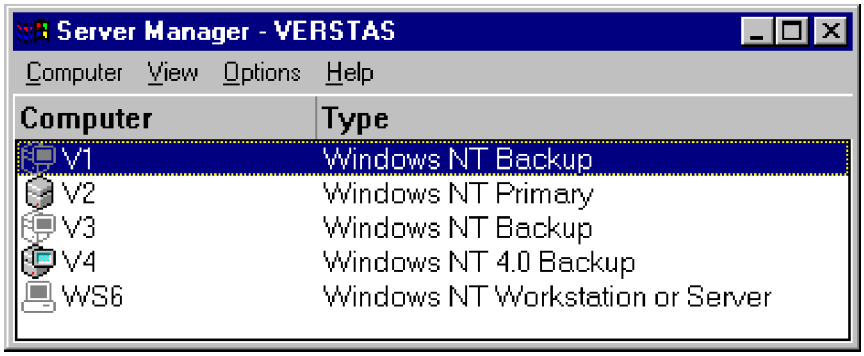
- Jos et ole aiemmin hallinnut määritettyä toimialuetta, työryhmää tai työasemaa/palvelinta, NT määrittää automaattisesti sopivan yhteystilan. Lisäksi se valitsee tai poistaa a.o. vaihtoehdon valinnan

- Jos käynnistät **Server Manager**in komentoriviltä, voit antaa komennon jälkeen hitaan yhteyden parametrin (**/L**) tai nopean yhteyden parametrin (**/H**). Jos esimerkiksi haluat hallita **HALLINTO**-toimialuetta hitaan tiedonsiirtoyhteyden kautta, anna komento **SRVMGR HALLINTO /L**.

Voit antaa komennon myös **Suorita** (Run)-komennon avulla ja fokusoida toimialueen sijasta suoraan haluttuun NT-työasemaan/palvelimeen komennolla **SRVMGR \\WS2**.

Toimialueen valitseminen

Kun **Server Manager** käynnistetään, ikkunassa näkyy se toimialue, johon käyttäjä on kirjautunut.



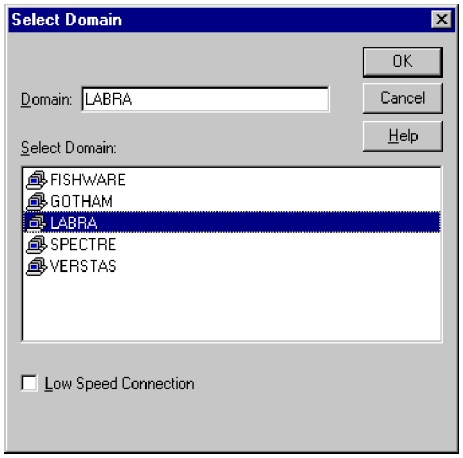
Computer | **Select Domain**-komennolla voit valita toisen toimialueen, NT-työryhmän (Workgroup) tai yksittäisen työaseman.

Voit vaihtaa toimialuetta seuraavasti:

1) Valitse **Computer** | **Select Domain**

2) Valitse toimialue **Select Domain**-luettelosta tai kirjoita sen nimi **Domain**-ruutuun; voit myös antaa **NT-työryhmän** kirjoittamalla työryhmän nimen; voit antaa **yksittäisen NT-työaseman/palvelimen** nimen kirjoittamalla **\\nimi**

3) Jos olet yhteydessä toimialueeseen, työryhmään tai työasemaan/palvelimeen **hitaan tiedonsiirtoyhteyden kautta** (esimerkiksi **RAS**), valitse vaihtoehto **Low Speed Connection**. NT tallentaa tämän asetuksen arvon 20 viimeksi tarkastellusta toimialueesta, työryhmästä tai **yksittäisestä NT-työasemasta/palvelimesta**. Kun annat nimen, asetuksen mahdollinen aiempi arvo tulee näkyviin. Jos aiempi asetus ei ole tiedossa, vaihtoehto ei aluksi ole valittuna. Voit hyväksyä asetuksen tai muuttaa sitä



4) Valitse lopuksi **OK**.

Käynnistämällä **Server Manager**in komentoriviltä voit fokusoida myös suoraan haluttuun kohteeseen. Jos haluat hallita **VERSTAS**-toimialuetta anna komento **SRVMGR VERSTAS**, jos haluat hallita NT-työasemaa **WS6** anna komento **SRVMGR \\WS6**.

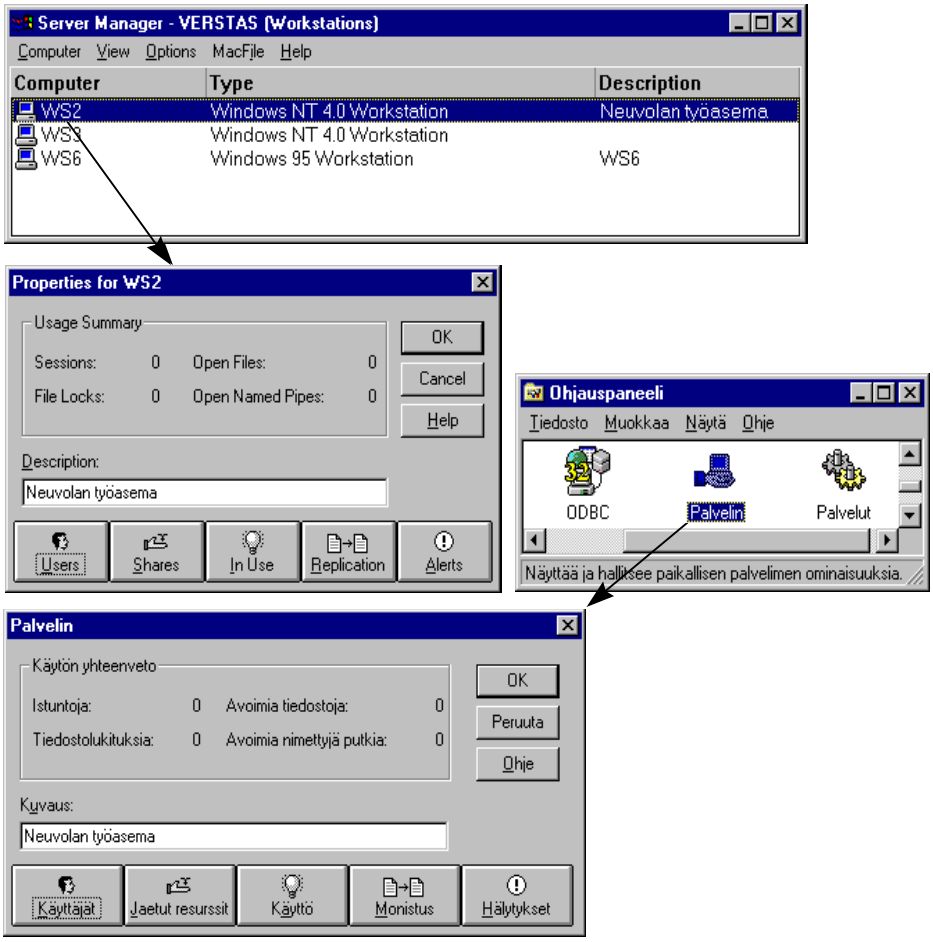
Palvelimen ominaisuudet

Palvelimen ominaisuuksien hallinta tehdään kaksoisnapauttamalla ikkunassa näkyvää NT-koneen nimeä tai valitsemalla ensin kohde ja sitten **Computer** | **Properties**.

Tämän jälkeen näyttöön tulee aivan sama ikkuna kuin käynnistettäessä NT-koneessa **Ohjauspaneelista** (Control Panel) **Palvelin** (Server)-kuvake.

Katso lisätietoja tämän kirjan **Ohjauspaneelia** käsittelevästä osasta, luku **3**.

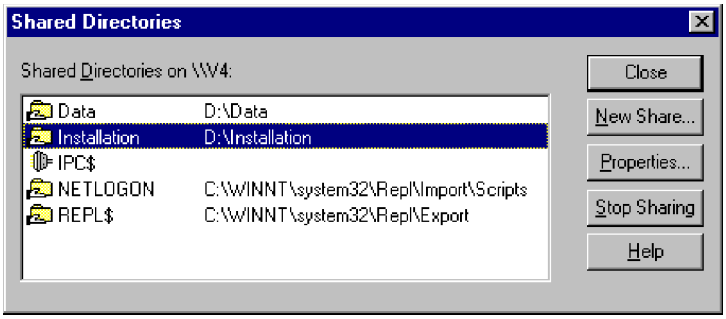
Tässä esimerkissä **Server Manager** on Windows NT:n englanninkielisestä versiosta ja Ohjauspaneelin **Palvelin** on suomenkielisestä versiosta:



Jaetut hakemistot

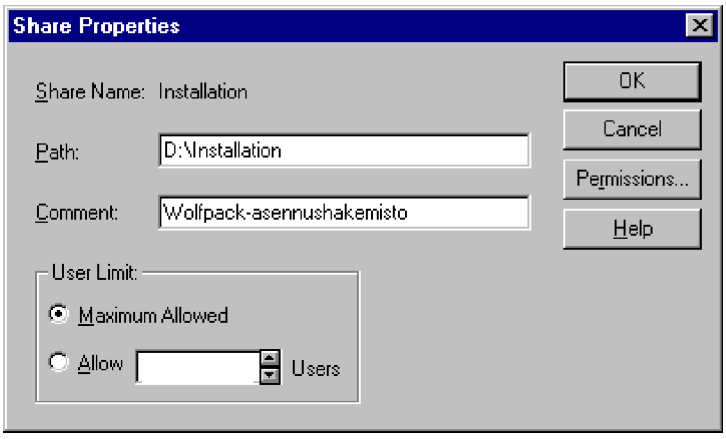
NT-koneen jaetun hakemiston ominaisuuksien hallinta tehdään seuraavasti:

1) Valitse ensin kohde ja sitten **Computer** | **Shared Directories**



2) Valitse jaettu hakemisto luettelosta

3) Valitse **Properties**-painike. Tämän jälkeen voit käsitellä jaetun hakemiston ominaisuuksia aivan kuten **Resurssienhallinnassa** (Explorer) tai **Tiedostonhallinnassa** (File Manager).

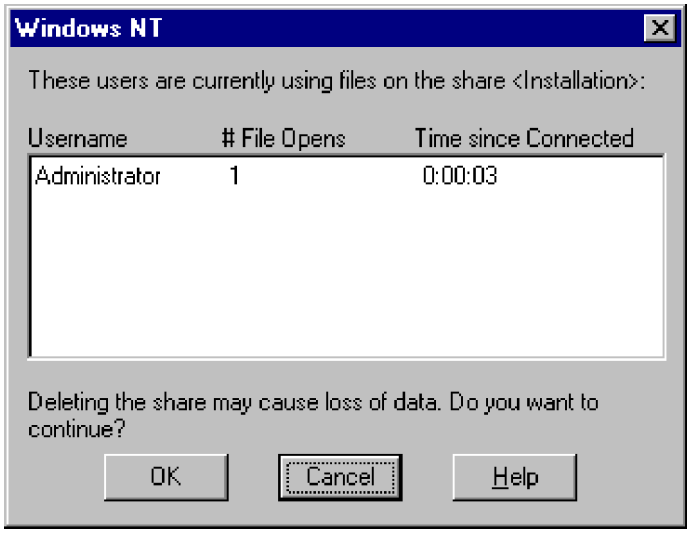


Painikkeella **Permissions** voit antaa käyttöoikeudet verkon kautta (**Access Through Share Permissions**).

Voit myös lisätä uuden jaetun hakemiston **New Share**-valinnalla. Tällöin hakemiston on oltava olemassa kyseisessä palvelimessa, ja resurssin polun on viitattava kyseiseen hakemistoon (kuten se palvelimella sijaitsee, ts. **D:\BUDJETTI**). Jälleen painikkeella **Permissions** voit antaa käyttöoikeudet jaetulle resurssille (**Access Through Share Permis-**

sions).

Voit lopettaa valitun hakemiston jakamisen **Stop Sharing**-valinnalla. Jos resurssilla on käyttäjiä, saat siitä ilmoituksen:

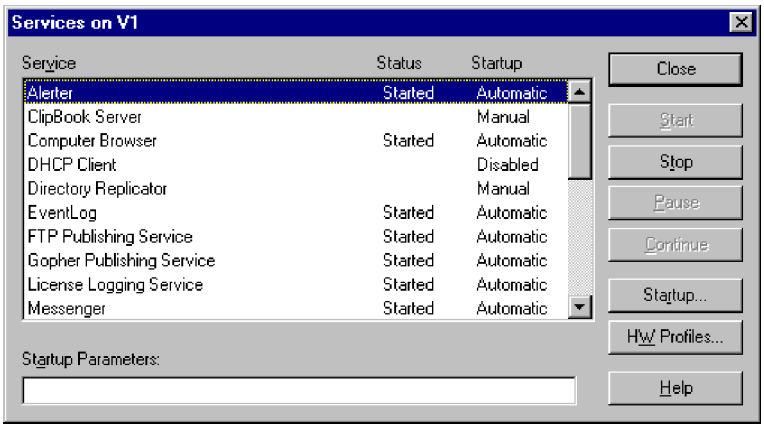


Palvelut

Valinnalla **Services** voi:

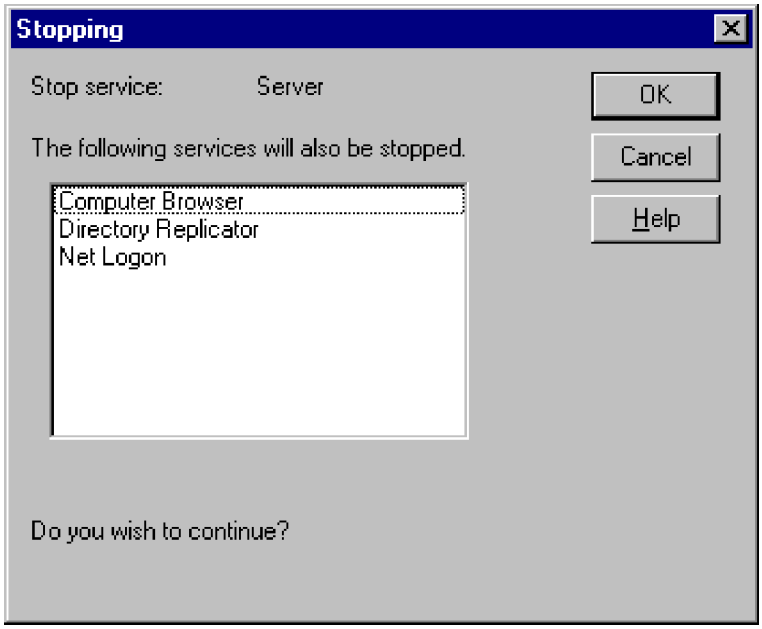
- Käynnistää, lopettaa tai keskeyttää halutun palvelun valitussa kohteessa
- Jatkaa palvelun käyttöä
- Välittää palvelulle käynnistysparametreja
- Määrittää palvelun kokoonpano

Katso lisätietoja tämän kirjan **Ohjauspaneelia** käsittelevästä osasta **luku 3**.



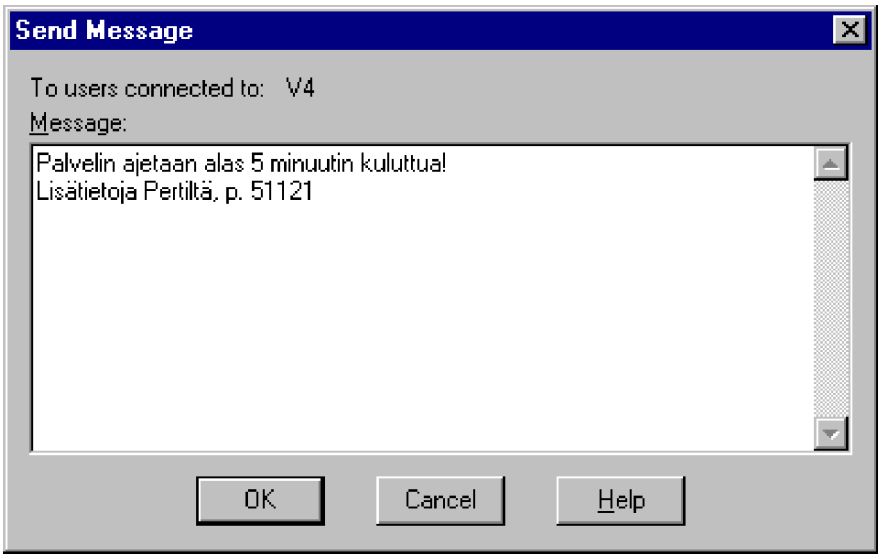
Pysäyttäessäsi palvelun saat ilmoituksen myös samalla lopetettavista palveluista.

Jos pysäytät **Server**-palvelun, et voi enää etähallita kohdetta!

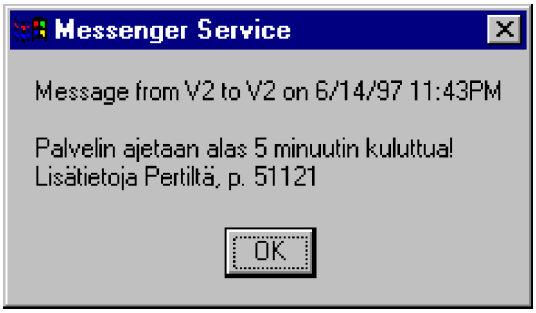


Viestien lähettäminen

Viestin lähettäminen yhteydessä oleville käyttäjille tehdään **Send Message**-komennolla. Valitse **Computer** | **Send Message**, kirjoita viesti **Message**-ruutuun ja paina **OK**.



Viesti ilmestyy palvelimeen kytkeytyneille käyttäjille:



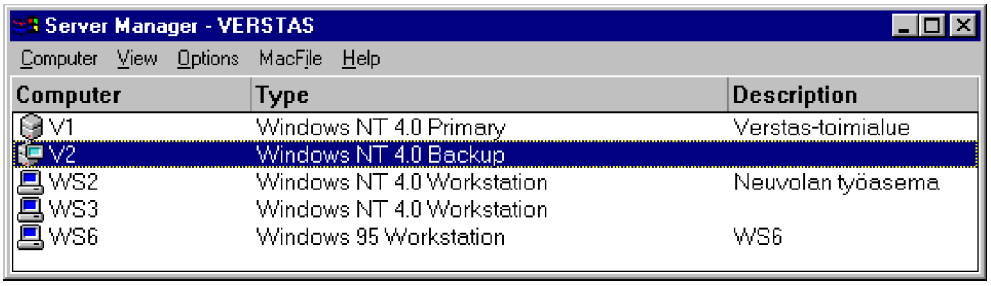
Palvelimen roolin muuttaminen

Palvelimen muuttaminen toimialueen **pääohjauskoneeksi** (*Primary Domain Controller*, PDC) tarkoittaa sitä, että toimialueen keskitetyt toiminnot (käyttäjätietokanta sekä PDC:n rooliin liittyvät palvelut) siirretään toimialueen toiseen palvelimeen, varaohjauskoneeseen (*Backup Domain Controller*, BDC). Tämä tilanne on tarpeen esimerkiksi vaihdettaessa tai päivitettäessä PDC:tä.

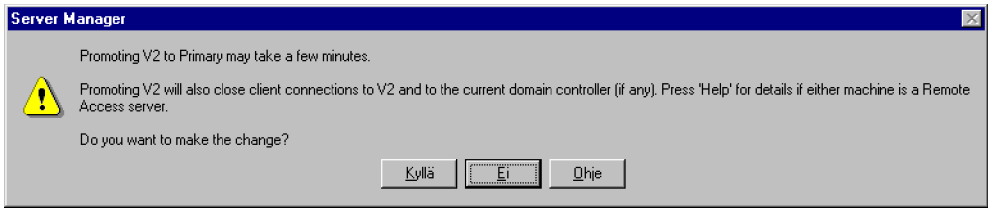
Toiminto tehdään seuraavasti:

1) Valitse kohteeksi haluttu BDC-palvelin, joka pystyy suorituskykyn-

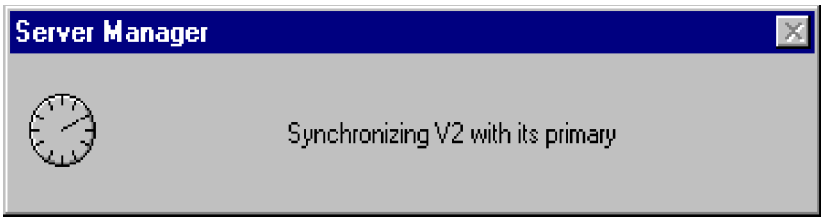
sä puolesta toimimaan PDC:nä. Esimerkissä palvelin **V2**:



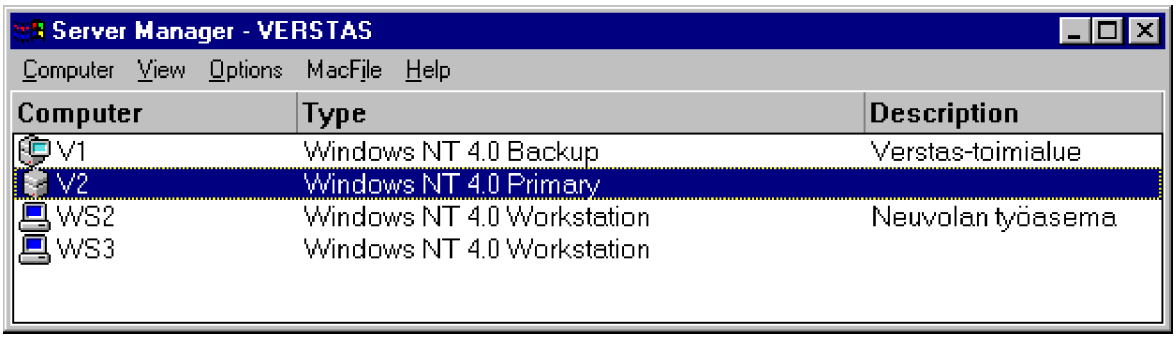
2) Valitse **Computer** | **Promote to Primary Domain Controller** - tätä et voi tehdä palvelimessa, joka jo on PDC. Hyväksy roolien muutos painamalla **Yes**:



Tämän jälkeen saat näyttöön ilmoitukset eri vaiheista, mitä palvelimen roolin muuttaminen aiheuttaa (Changing X's role to Primary, Synchronizing Z with its primary jne).



Lopulta voit tarkistaa, että rooli myös muuttui.



Huomaa:

- Tilanteessa, jossa toimialueella on vain PDC, voit vaikkapa asentaa tehokkaan työaseman BDC:ksi ja muuttaa näiden roolit huollon ajaksi

- Sillä aikaa kun rooleja muutetaan, NetLogon-palvelu ei ole käynnissä eikä toimialueen käyttäjätietokantaan voi tehdä muutoksia. Jos roolien muuttaminen kestää kauan (hidas verkko ja/tai suuri käyttäjätietokanta), toimialueella olisi hyvä olla toinenkin BDC joka tällä aikaa voi käsitellä verkkoonkir-

jautumispyynnöt

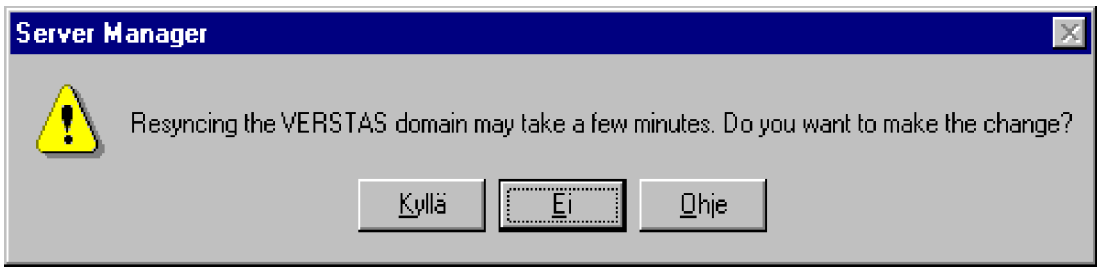
- Jos PDC ei ole verkossa, voit silti muuttaa minkä tahansa BDC:n PDC:ksi. Tällöin toimialueen käyttäjätietokanta tulee olemaan kyseisen BDC:n kopio toimialueen käyttäjätietokannasta

- Jos PDC myöhemmin tulee verkkoon, tilanteesta saattaa tulla pulmallinen. Se ei todennäköisesti pääse toimialueelle ollenkaan, joten sille on ensin tehtävä BDC:n konetunnus toimialueelle.

Käyttäjätietokannan synkronointi

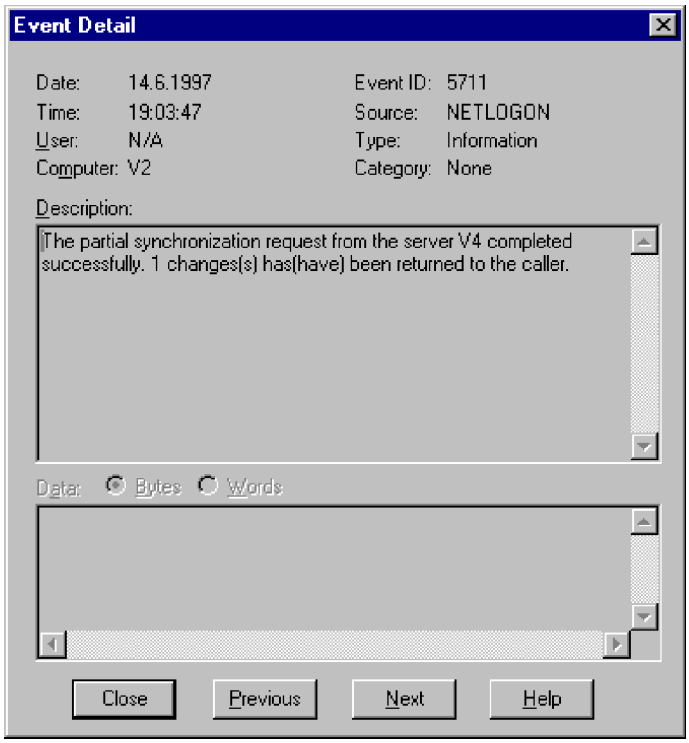
Toimialueen kaikkien palvelimien käyttäjätietokantojen (SAM ja LSA) synkronointi tehdään automaattisesti NetLogon-palvelun avulla. Jos toimialueen PDC:n ja muiden palvelimien käyttäjätietokannat eivät kuitenkaan tahdistu, voit tarvittaessa tahdistaa palvelimet valitsemalla ensin toimialueen PDC:n (ohjauskone) ja sitten **Computer** | **Synchronize Entire Domain**, jolloin toimialueen käyttäjätietokanta kopioidaan PDC:stä toimialueen BDC-palvelimiin.

Hyväksy toiminto painamalla **Yes**:

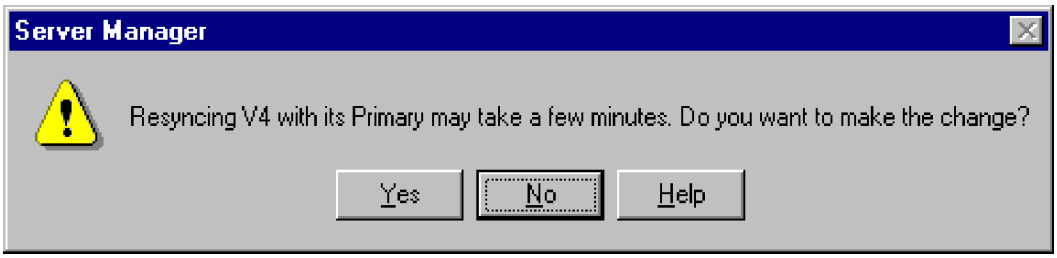


Saat ilmoituksen operaation käynnistymisestä:

Voit tarkistaa **Event Viewer**in järjestelmälokista, onko päivitys onnistunut:

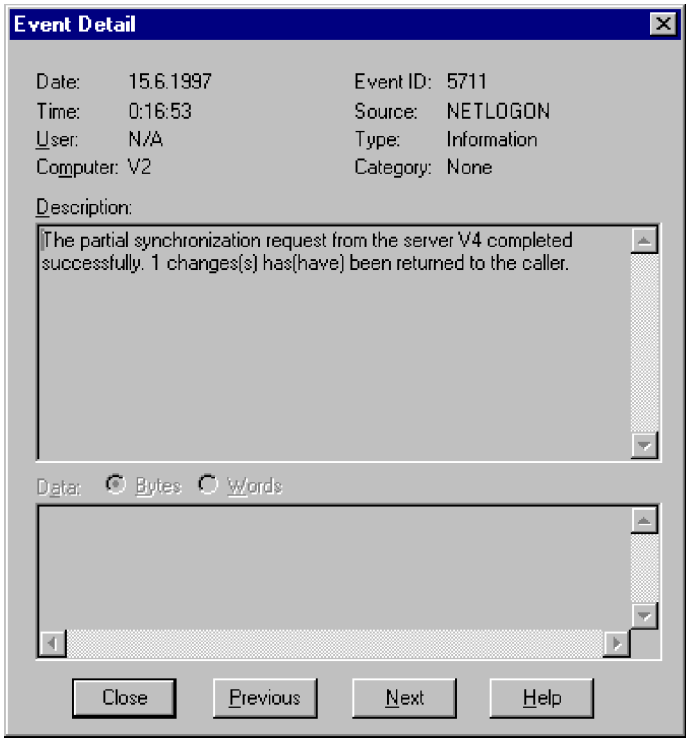


Yksittäisen palvelimen synkronointi toimialueen PDC:n kanssa tarvitaan, jos käyttäjätietokantaa ei saada synkronoitua automaattisesti tai jos **LAN Manager 2.x** -version palvelin ei pysty muodostamaan verkkoyhteyksiä. Se tehdään valitsemalla ensin haluttu palvelin ja sitten **Computer | Synchronize with Primary Domain Controller**.



Vastaa kysymykseen **Yes**.

Tämän jälkeen voit tarkistaa palvelimen järjestelmälokista Event Viewerilla, onko synkronointi onnistunut.



Tässä tapauksessa onnistui.

NT-koneen lisääminen toimialueelle

NT-työasema tai -palvelin on **lisättävä toimialueelle** ennen kuin se voi olla toimialueen täysivaltainen jäsen ja osa toimialueen suojausjärjestelmää.

Toimialueelle lisätyille työasemille/palvelimille on annettava **tunnus** toimialueen suojaustietokannassa. Työasemia/palvelimia voi lisätä toimialueelle kolmellakin tavalla:

1) Asennuksen yhteydessä

2) **Järjestelmänvalvoja** (Administrator) voi lisätä aiemmin asennetun NT-työaseman toimialueelle käyttämällä työaseman **Ohjauspaneelin** (Control Panel) **Verkko** (Network)-kuvaketta

3) **Server Manager**in **Computer** | **Add to Domain**-komennolla ja lisäksi käyttämällä kyseisen NT-työaseman **Ohjauspaneelin** (Control Panel) **Verkko** (Network)-kuvaketta.

Lisätty **tunnus** on oleellisesti tietosuojaan vaikuttava tekijä. Ennen kuin tunnuksen saanut NT-kone liittyy toimialueelle, joku toinen käyttäjä voi antaa toiselle NT-koneelle saman tunnuksen ja liittää sen toimialueelle käyttäen aiemmin luotua tunnusta. Jos liitetty NT-kone on palvelin, se saa liittyessään kopion toimialueen käyttäjätietokannasta!

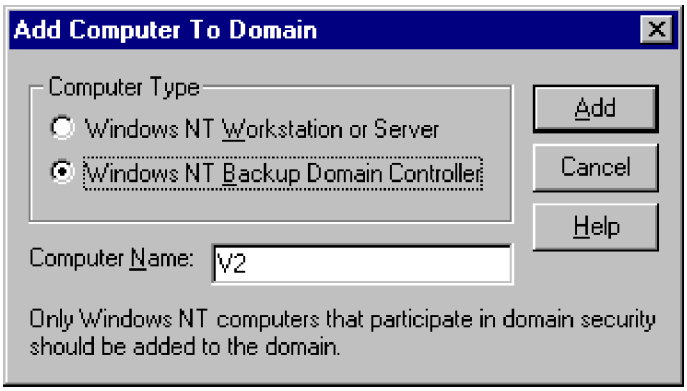
Tietokoneen lisääminen toimialueelle edellyttää, että olet kirjautunut järjestelmään **Administrators**-, **Domain Admins**- tai **Account Operators** -ryhmän jäsenenä.

Lisääminen tehdään seuraavsti:

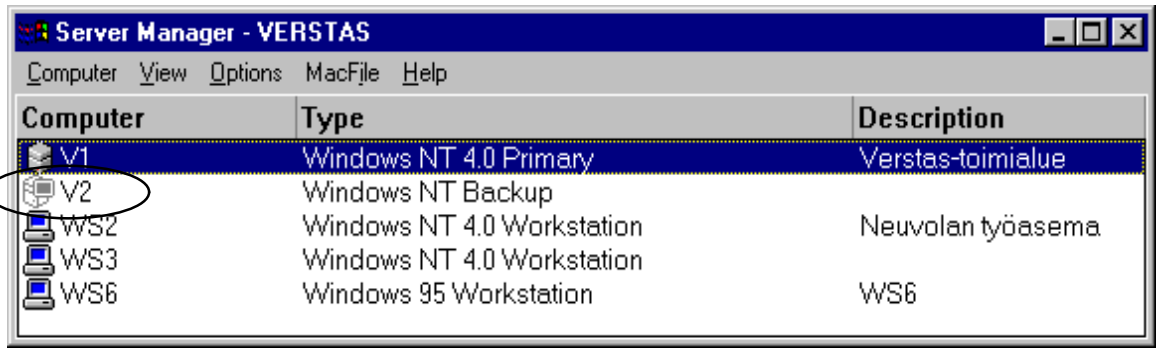
1) Valitse **Computer** | **Add to Domain**. Valitse joko **Windows NT Workstation or Server** tai **Windows NT Backup Domain Controller**

2) Kirjoita tunnus **Computer name** -ruutuun ja valitse **Add**-painike. NT lisää tunnusta vastaavan tilin toimialueen tietokantaan

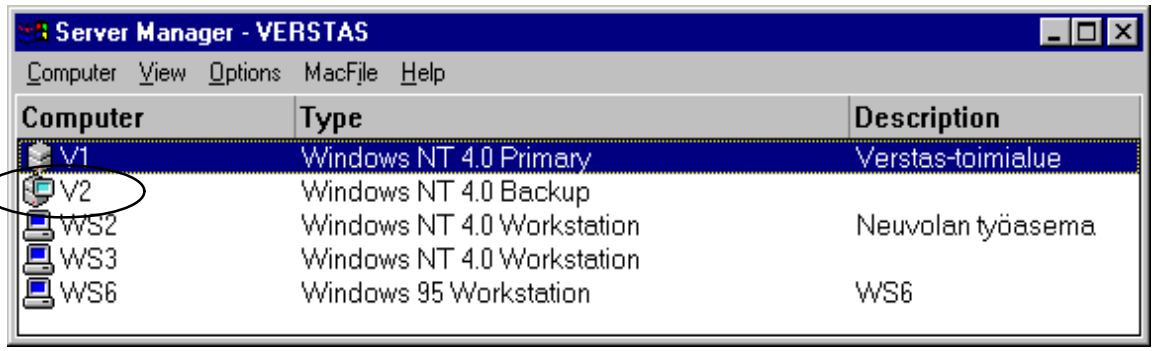
3) Valitse lopuksi **Close**-painike.



NT lisää työaseman/palvelimen **Palvelimen hallinnan** (Server Manager) luetteloon. Kuvake on himmeä eikä työasemalla/palvelimella ole myöskään versionumeroa eikä kuvausta, ennen kuin sen käyttäjä liittyy toimialueelle. NT-palvelin **V2** on lisätty toimialueelle, mutta se ei ole vielä ilmoittanut itsestään...



Kuvake ei ole enää himmeä ja nyt nähdään myös versionumero:



NT-työaseman kuuluminen työryhmään tai toimialueelle asetetaan **Ohjauspaneelista** (Control Panel) **Verkko** (Network)-kuvakkeen **Tunnistus** (Identification)-välilehden asetusten avulla. Oletuksena asennuksen yhteydessä NT-työasemat kuuluvat **Työryhmä** (Workgroup)-nimiseen työryhmään. Onnistuneesta työaseman liittämisestä toimialueelle tulee käyttäjälle ilmoitus **Tervetuloa toimialueelle...** (Welcome to domain...). Jos näin ei käy, seuraavassa vinkkejä:

- Jos haluat siirtää NT-työaseman toimialueelta toiselle, muuta ensin työasema mihin tahansa työryhmään, vaikkapa **SPECTRE**. Käynnistä NT-työasema uudelleen ja muuta sitten toimialue oikeaksi

- Työasemasta ei saa olla verkkoyhteyksiä palvelimiin muutoksen aikana! Voit komentoriviltä sulkea kaikki verkkoyhteydet komennolla **NET USE * /D**. Lopeta lisäksi kaikki käyttämäsi sovellukset.

NT-koneen poistaminen toimialueelta

Kun NT-kone on poistettu toimialueelta, se ei enää kuulu toimialueen suojausjärjestelmään ja kyseisen NT-koneen tunnus poistetaan toimialueen suojaustietokannasta.

Poistaminen tehdään valitsemalla ensin poistettava työasema/palvelin (PDC:tä et voi poistaa) ja **Computer** | **Remove from Domain**.
Voit myös painaa **Delete**:

Vastaa kysymykseen **Yes**.

Muuta asetukset NT-työasemassa **Ohjauspaneelin** (Control Panel) **Verkko** (Network)-kuvakkeen avulla ja anna jonkin toisen toimialueen tai työryhmän nimi.

NT-koneen nimen muuttaminen

NT-koneen nimen muuttaminen tehdään valitsemalla **Computer** | **Add to Domain** ja antamalla tarvittavat tiedot. Kirjoita tähän valintaikkunaan uusi työaseman nimi ja muuta työaseman nimi **Ohjauspaneelin** (Control Panel) **Verkko** (Network)-kuvakkeen avulla.
Valitse vanha nimi **Server Manager**-ikkunan luettelosta ja valitse **Computer** | **Remove from Domain**.

Muista:

- Ei ole suositeltavaa muuttaa PDC:n nimeä!
- Et voi välttämättä muuttaa ohjauskoneita toimialueelta toiselle ilman uudelleenasennusta!
- Et voi muuttaa Server-tyyppisen palvelimen roolia, mutta toimialuetta voit!

Toimialueen nimen muuttaminen

Seuraavan(kin) tempun voi tehdä omalla vastuulla. Toimialueen nimen muuttaminen tehdään seuraavasti:

1) Varmista, ettei uudelleennimettävällä toimialueella ole käyttäjiä

2) Kirjaudu PDC-palvelimeen ja katkaise luottosuhteet toisiin toimialueihin

3) Muuta toimialueen nimi BDC-palvelimissa. Sammuta palvelimet

4) Tee toimialueen nimen muutos PDC-palvelimessa ja käynnistä se uudelleen. Odota muutamia minuutteja (kunnes selauspalvelu on käynnistynyt)

5) Käynnistä nyt BDC:t

6) Määrittele luottosuhteet uudelleen toisiin toimialueisiin

7) Siirrä NT-työasemat uuteen toimialueeseen **Ohjauspaneelin** (Control Panel) **Verkko** (Network)-kuvakkeen avulla. Vaikka Työryhmä-Windowsissa ja Windows 95:ssä kirjautumisikkunassa voi antaa vanhan toimialueen sijasta uuden toimialueen nimen, niin työryhmän määrittely uudelleen on kuitenkin tyylikkäintä. Tällä nimittäin varmistetaan selauspalvelun toiminta.

Palvelimien hallinta NET-komentojen avulla

Voit käyttää komentorivin **NET-komentoja** palvelimien hallinnassa.

NET ACCOUNTS

Voit synkronoida käyttäjätietokannan (*Account Database*) **NET ACCOUNTS**-komennon avulla.

Komento **NET ACCOUNTS /SYNC** toimialueen PDC:ssä annettuna synkronoi toimialueen kaikkien palvelinten käyttäjätietokannan PDC:n kanssa. BDC:llä käytettynä synkronoi kyseisen palvelimen käyttäjätietokannan toimialueen PDC:n kanssa.

NET COMPUTER

Lisää/poistaa tietokoneen toimialueen tietokannasta; tämä komento on käytettävissä vain Windows NT Servereissä.

Syntaksi:

NET COMPUTER \\TIETOKONENIMI {/ADD | /DEL}

Parametrit:

\\TIETOKONENIMI	Toimialueelle lisättävä tai siltä poistettava tietokone
/ADD	Lisää tietokoneen toimialueelle
/DEL	Poistaa tietokoneen toimialueelta.

Komento

NET COMPUTER V7 /ADD

lisää toimialueelle konetunnuksen **V7**-nimiselle NT-työasemalle tai **Stand-alone Serverille**.

NET CONFIG SERVER

Näyttää tai muuttaa palvelinpalvelun parametreja, jos palvelu on käynnistetty. Muutokset tulevat voimaan heti ja ovat pysyviä. Osaa palvelinpalvelun määrityksistä ei voi muuttaa **NET CONFIG SERVER** -komennolla; ne näet kuitenkin komennon avulla. Suomenkielisessä versiossa myös komento **NET CONFIG PALVELIN** toimii.

Komento tuo näyttöön:

- palvelimen nimen verkossa
- palvelinta kuvaavan kommentin
- ohjelmiston versiotiedot
- verkon kuvauksen
- palvelimen piilotuksen
- tilan
- palvelimen jaettuja resursseja käyttävien käyttäjien enimmäismäärän
- palvelimella avoinna olevien tiedostojen enimmäismäärän
- istuntojen odotusaika -asetuksen

Syntaksi:

NET CONFIG SERVER [/AUTODISCONNECT:AIKA] [/SRVCOMMENT:"TEKSTI"] [/HIDDEN:{YES | NO}]

Parametrit:

ei mitään — Näyttää palvelinpalvelun nykyiset määritykset

/AUTODISCONNECT:AIKA — Määrittää ajan, jonka kuluttua passiivinen istunto katkaistaan. Jos arvo on **-1**, passiivisia istuntoja ei katkaista; sallitut arvot ovat **-1 - 65535** minuuttia; oletusarvo on **15** minuuttia

/SRVCOMMENT:"TEKSTI" — Lisää kommentin, joka näytetään palvelimen kohdalla NT:n näytöissä ja **NET VIEW** -komennolla. Kommentissa voi olla

enintään 48 merkkiä ja kirjoita teksti lainausmerkkeihin

/HIDDEN:{YES | NO} Määrittää, näytetäänkö palvelimen tietokonenimi palvelinluetteloissa. Huomaa, että palvelimen piilottaminen ei vaikuta sen käyttöoikeuksiin. Oletusarvo on **no** eli tietokonenimi näytetään.

Voit tuoda näyttöön palvelimen tiedot ruutu kerrallaan komennolla:

NET CONFIG SERVER | MORE

Voit estää palvelimen nimen näkymisen selauslistalla komennolla:

NET CONFIG SERVER /HIDDEN:YES

Voit asettaa järjestelmän katkaisemaan automaattisesti käyttäjien istunnot, jotka ovat olleet käyttämättä 60 minuutin ajan komennolla:

NET CONFIG SERVER /AUTODISCONNECT:60

NET CONFIG WORKSTATION

Näyttää / muuttaa **Workstation**-palvelun parametreja, jos palvelu on käynnistetty. Myös komento **NET CONFIG RDR** toimii, suomenkielisessä versiossa myös komento **NET CONFIG TYÖASEMA** toimii.

Syntaksi:

NET CONFIG WORKSTATION [/CHARCOUNT:TAVUA] [/CHARTIME:MILLISEKUNTIA] [/CHARWAIT:SEKUNTIA]

Parametrit:

ei mitään Näyttää työaseman nykyiset määritykset

/CHARCOUNT:TAVUA Tavumäärä, joka kerätään, ennen kuin tiedot lähetetään. Jos myös parametri **/CHARTIME:MILLISEKUNTIA** on määri-

tetty, tavut lähetetään heti, kun toinen ehdoista täyttyy. Sallitut arvot ovat **0 - 65535** tavua; oletusarvo on **16 tavua**

/CHARTIME:MILLISEKUNTIA Määrittää ajan, joka tietoja kerätään,ennen kuin ne lähetetään. Jos myös **/CHARCOUNT:TAVUA** on käytössä, tiedot lähetetään heti, kun toinen ehdoista täyttyy; sallitut arvot ovat **0 - 655350000** millisekuntia ja oletusarvo on **250** millisekuntia

/CHARWAIT:SEKUNTIA Odotusaika **sekuntia** käytetyn tietoliikennelaitteen vapautumiselle; arvot ovat **0 - 65535**; oletusarvo on 3600 sekuntia.

NET CONTINUE

Jatkaa keskeytettyjä palveluita.

Syntaksi:

NET CONTINUE PALVELU

Parametrit:

palvelu Jatkettava palvelu voi olla NT:n versiosta riippuen jokin seuraavista:

- **FILE SERVER FOR MACINTOSH**
- **SCHEDULE**
- **FTP SERVER**
- **LPDSVC**
- **NET LOGON**
- **NETWORK DDE**
- **NETWORK DDE DSDM**
- **NT LM SECURITY SUPPORT PROVIDER**
- **REMOTEBOOT**
- **REMOTE ACCESS SERVER**
- **SERVER**
- **SIMPLE TCP/IP SERVICES**
- **WORKSTATION**

NET FILE

Komennolla voit tarkastella ja valvoa verkossa jaettuja tiedostoja. Jaetut tiedostot saattavat joskus jäädä vahingossa avoimiksi ja lukituiksi, jolloin työasemat eivät voi käyttää tiedoston lukittuja osia. Voit poistaa lukituksen ja sulkea tiedoston käyttämällä valitsinta **/CLOSE**. Näet myös palvelimella avoinna olevien tiedostojen nimien lisäksi - jos niitä on - tiedostolukitusten määrän kullekin tiedostolle.

Syntaksi:

NET FILE [TUNNUS [/CLOSE]]

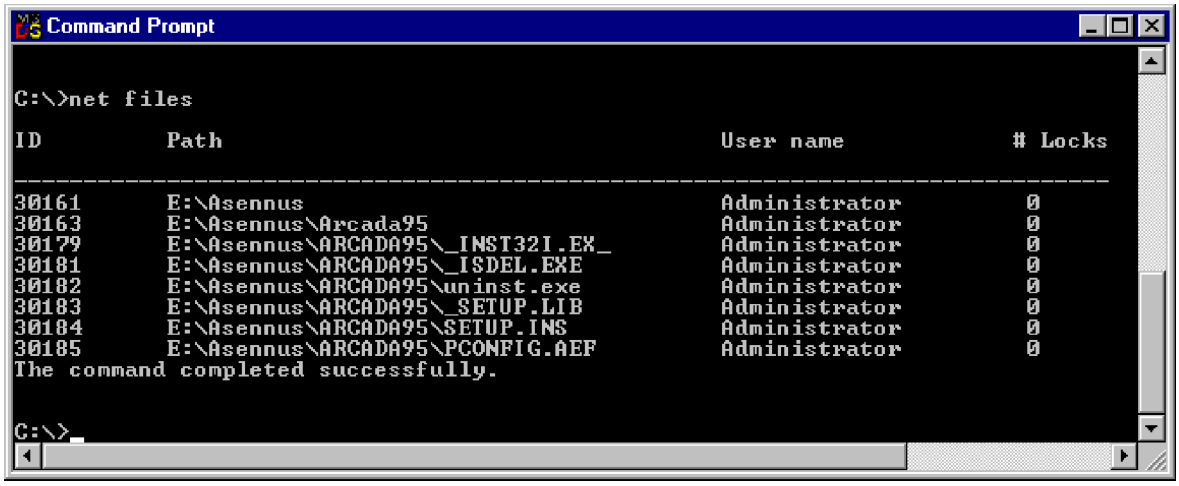
Parametrit:

ei mitään Palvelimella avoinna olevien tiedostojen nimet

tunnus Tiedoston tunnusluku

/close Sulkee avoimen tiedoston ja poistaa lukitukset. Anna komento palvelimella, jolla jaettu tiedosto on

Komento voidaan kirjoittaa myös muodossa **NET FILES**:



NET NAME

Lisää tai poistaa viestinimen tai näyttää nimet, joille lähetetyt viestit NT-kone ottaa vastaan. **Messenger**-palvelun on oltava käynnissä, jotta komentoa voitaisiin käyttää.

Syntaksi:

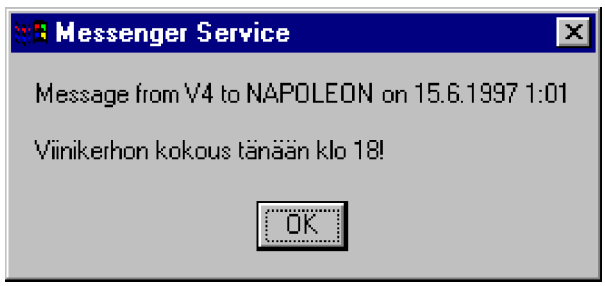
NET NAME [NIMI [/ADD | /DELETE]]

Parametrit:

Ei mitään	Näyttää käytössä olevat nimet
NIMI	Määrittää nimen, jolle lähetetyt viestit otetaan vastaan; se voi olla enintään **15** merkkiä pitkä
/ADD	Lisää nimen työasemaan. Parametri **/ADD** on valinnainen, net name nimi toimii samalla tavalla kuin **NET NAME NIMI /ADD**
/DELETE	Poistaa nimen työasemasta

Esimerkiksi lisätään työasemaan nimi **Napoleon**:

Tämän jälkeen voidaan lähettää viesti kyseiselle nimelle:



NET PAUSE

Keskeyttää käynnistetyn palvelun toistaiseksi.

Syntaksi:

NET PAUSE PALVELU

Parametrit:

Palvelu Palvelu voi olla NT:n versiosta ja asennuksesta riippuen jokin seuraavista:

- **FILE SERVER FOR MACINTOSH**
- **SCHEDULE**
- **FTP SERVER**
- **LPDSVC**
- **NET LOGON**
- **NETWORK DDE**
- **NETWORK DDE DSDM**
- **NT LM SECURITY SUPPORT PROVIDER**
- **REMOTEBOOT**
- **REMOTE ACCESS SERVER**
- **SERVER**
- **SIMPLE TCP/IP SERVICES**
- **WORKSTATION**

NET PRINT

Näyttää tai hallitsee tulostustöitä ja tulostusjonoja.

NET PRINT \\PALVELIN\TULOSTUSJONO
NET PRINT [\\PALVELIN] TYÖNUMERO [/HOLD | /RELEASE | /DELETE]

Parametrit

PALVELIN	Palvelin, jolla jaetut tulostusjonot ovat
TULOSTUSJONO	Tulostusjonon nimi
työnumero	Tulostusjonossa olevalle työlle annettu tunnusnumero. Työnumero on yksilöllinen. Samaa numeroa ei anneta uudelleen edes saman palvelimen eri tulostusjonoissa oleville töille
/hold	Työnumeron kanssa käytettynä keskeyttää määritetyn tulostustyön. Työ pysyy jonossa ja muut työt ohittavat sen, kunnes työn käsittelyä jatketaan **/RELEASE**-komennolla
/release	Jatkaa keskeytettyä tulostustyötä
/delete	Poistaa työn tulostusjonosta

Esimerkkejä:

Voit keskeyttää palvelimen **HP** tulostustyön **126** komennolla:
NET PRINT \\HP 126 /HOLD

Saat näyttöön palvelimen **HP** tulostusjonon **4M** komennolla:
NET PRINT \\HP\4M

NET SEND

Lähettää viestejä käyttäjille, työasemille, palvelimille tai viestinimille. Viestejä voidaan ottaa vastaan vain, jos **Messenger**-palvelu on käynnissä.

Syntaksi:

NET SEND {NIMI | * | /DOMAIN[:NIMI] | /BROADCAST | /USERS} VIESTI

Parametrit:

nimi	Käyttäjänimi, tietokoneen nimi tai viestinimi, jolle viesti lähetetään. Jos nimi on välilyöntejä sisältävä tietokonenimi, se on pitää kirjoittaa "lainausmerkkeihin"
*	Lähettää viestin kaikille ryhmääsi kuuluville nimille
/domain[:nimi]	Lähettää viestin kaikille nimille toimialueella, johon työasema kuuluu. Jos nimi on määritetty, viesti lähetetään kaikille määritetyn toimialueen tai työryhmän nimille
/broadcast	Lähettää viestin koko verkon kaikille nimille. Vain Järjestelmänvalvojat (Administrators)-ryhmän jäsenillä on käyttöön tarvittavat oikeudet
/USERS	Lähettää viestin kaikille käyttäjille, joilla on yhteys palvelimeen
VIESTI	Lähetettävä sanoma.

Esimerkkejä - viesti kaikille saman toimialueen käyttäjille:
NET SEND /USERS "Palvelin ajetaan alas klo 22!"

Viesti työaseman **WS2** käyttäjälle:
NET SEND \\WS2 "Lopetetaanpas se Doomin pelaaminen!”

Viesti Administrator -käyttäjätunnukselle:
NET SEND ADMINISTRATOR "Mikä oli ActiveX-rompun CD-KEY?”

NET SESSION

Luettelee palvelimen ja siihen yhdistettyjen työasemien väliset istunnot tai lopettaa ne.

Syntaksi:

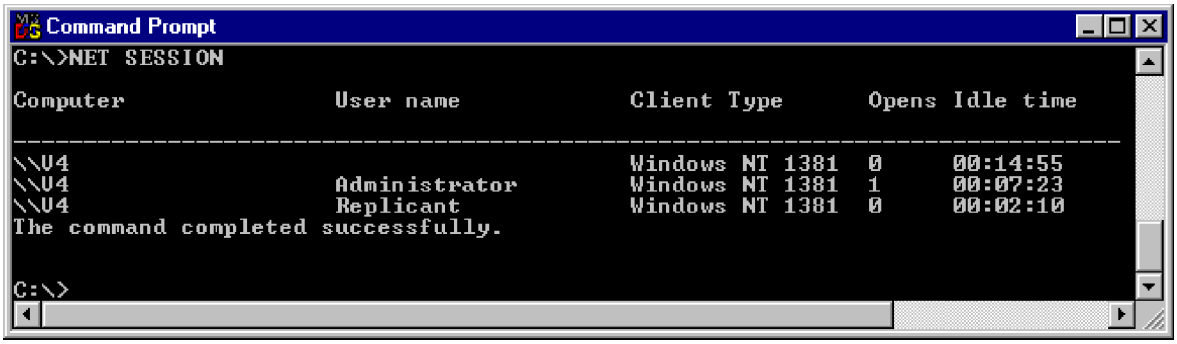
NET SESSION [\\TYÖASEMA][/DELETE]

Parametrit:

ei mitään	Palvelimen kaikkien istuntojen tiedot
\\TYÖASEMA	NT-kone, jonka istunnot luetellaan tai lopetetaan
/DELETE	Lopettaa **\\TYÖASEMA** istunnon palvelimella ja sulkee kaikki kyseisessä istunnossa palvelimella avatut tiedostot. Jos argumenttia ei ole määritetty, kaikki istunnot palvelimella lopetetaan

Esimerkki:

NET SESSION



NET SHARE

Luo, poistaa ja näyttää jaettuja resursseja.

Syntaksi:

NET SHARE JAKONIMI

NET SHARE JAKONIMI=ASEMA:POLKU [/USERS:MÄÄRÄ|/UNLIMITED] [/REMARK:"TEKSTI"]

NET SHARE JAKONIMI [/USERS:MÄÄRÄ | UNLIMI-TED][/REMARK:"TEKSTI"]

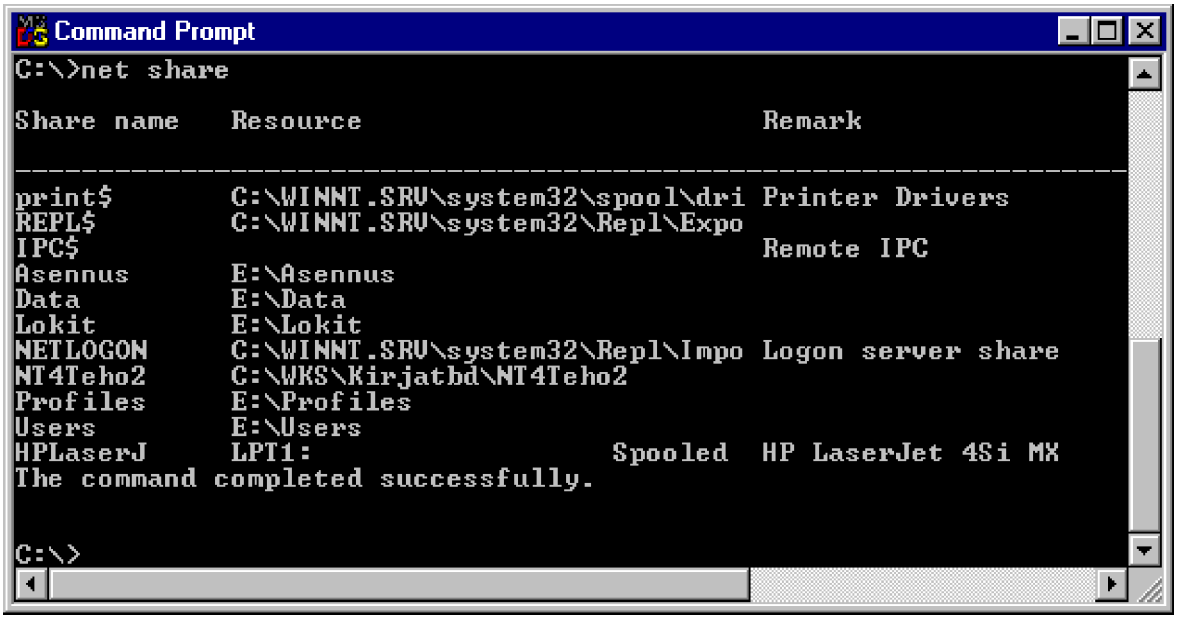
NET SHARE {JAKONIMI|ASEMA:POLKU}/DELETE

Parametrit:

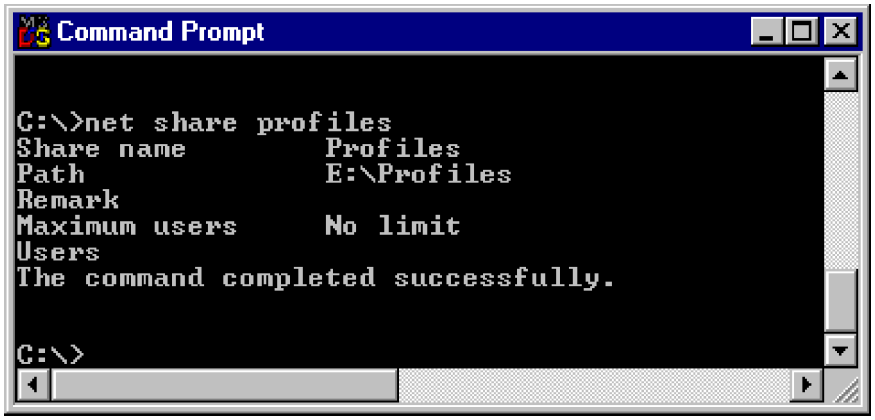
ei mitään	Näyttää paikallisen palvelimen kaikkien jaettujen resurssien tiedot
JAKONIMI	Jaetun resurssin verkkonimi. Saat tietoja palvelinalueesta kirjoittamalla **NET SHARE \\jakonimi**
asema:polku	Polku jaettavaan hakemistoon
/users:määrä	Jaettua resurssia samanaikaisesti käyttävien käyttäjien enimmäismäärä
/unlimited	Samanaikaisesti resurssia käyttävien käyttäjien lukumäärää ei ole rajoitettu
/remark:"teksti"	Määrittää resurssia kuvaavan kommentin - kirjoita teksti "lainausmerkkeihin"
/delete	Lopettaa resurssin jakamisen.

Esimerkkejä:

Komento luettelee kaikki jaetut resurssit: järjestelmäresurssit ja juurihakemistot jaetaan piilotettuina $-merkillä:



NET SHARE jakonimi -komennolla näet tarkemmin tietoja jaetuista resursseista:



Esimerkki hakemiston jakamisesta komentojonon avulla. Luodaan ja jaetaan **PUB**-hakemisto NTFS-levyltä sekä annetaan hakemistoon täydet oikeudet **Users**-ryhmälle; poistetaan **Everyone**-ryhmän oikeudet:

```
D:
MD HALLINTO
MD HALLINTO\PUB
NET SHARE PUB=D:\HALLINTO\PUB /USERS:5 /REMARK:TALLENNUS
CACLS D:\HALLINTO\PUB /E /R EVERYONE
CACLS D:\HALLINTO\PUB /E /G USERS:F
```

Komentojono, joka poistaa jaon (sitten voidaan ottaa vaikka varmistus hakemistosta) ja jakaa hakemiston uudelleen. Tämä voitaisiin vaikka ajastaa **AT**-komennolla:

```
NET SHARE PUB /D
... varmistuskopiointi ...
NET SHARE PUB=D:\HALLINTO\PUB /USERS:5 /REMARK:TALLENNUS
```

NET START

Käynnistää palvelun tai tuo näyttöön luettelon käynnistetyistä palveluista. Jos palveluiden nimet muodostuvat useammasta kuin yhdestä sanasta, ne on kirjoitettava "lainausmerkkeihin".

Syntaksi:

```
NET START [PALVELU]
```

Parametrit:

ei mitään Käynnistettyjen palveluiden luettelo; palveluiden nimet riippuvat asennetuista palveluista ja voivat olla: ALERTER, CLIENT SERVICE FOR NETWARE, CLIPBOOK SERVER, COMPUTER BROWSER, DHCP CLIENT, DIRECTORY REPLICATOR, EVENTLOG, FTP SERVER, LPDSVC, MESSENGER, NET LOGON, NETWORK DDE, NETWORK DDE DSDM, NETWORK MONITORING AGENT, NT LM SECURITY SUPPORT PROVIDER, REMOTE ACCESS CONNECTION MANAGER, REMOTE ACCESS ISNSAP SERVICE, REMOTE ACCESS SERVER, REMOTE PROCEDURE CALL (RPC) LOCATOR, REMOTE PROCEDURE CALL (RPC) SERVICE, SCHEDULE, SERVER, SIMPLE TCP/IP SERVICES, SNMP, SPOOLER, TCPIP NETBIOS HELPER, UPS, WORKSTATION

Esimerkiksi käynnistetään etäkäyttöpalvelinpalvelu:
NET START "REMOTE ACCESS SERVER"

IIS:n WWW-palvelimen käynnistys:
NET START “WORLD WIDE WEB PUBLISHING SERVICE”

NET STATISTICS

Näyttää paikallisen työaseman tai palvelimen tilastolokin.

Syntaksi:

NET STATISTICS [TYÖASEMA | PALVELIN]

NET STATISTICS [WKSTA | SERVER]

Parametrit:

ei mitään Näyttää luettelon käynnissä olevista palveluista, joista on saatavana tilastotietoja

työasema Näyttää paikallisen työaseman tilastot

palvelin Näyttää paikallisen palvelimen tilastot.

Esimerkiksi tallennetaan tilastotiedot palvelimen nimellä palvelimen **HAL9000** jakamaan **LOGS**-hakemistoon:
NET STATS SRV > \\HAL9000\LOGS\%COMPUTERNAME%.LOG

NET STOP

Pysäyttää Windows NT:n halutun verkkopalvelun.

Syntaksi:

NET STOP PALVELU

Parametrit:

palvelu Ks. NET START-komennon kohdalta

Esimerkki palveluiden pysäyttämisestä ja käynnistämisestä vaikkapa varmistuskopioinnin ajaksi:

```
NET STOP SERVER /Y
-- halutut toiminnot --
NET START SERVER
NET START "COMPUTER BROWSER"
NET START NETLOGON
```

NET STOP SERVER pysäyttää myös NetLogon- ja selauspalvelun, mutta ei käynnistä niitä automaattisesti. Siksi ne on käynnistettävä erikseen. Komentojono, joka pysäyttää **SQL Server**in, kutsuu **SQLBACK.CMD**-komentojonoa (se voisi olla SQL Serverin tietokannat nauhalle varmistava komentojono) ja käynnistää SQL Serverin uudelleen.

```
NET STOP MSSQLServer
CALL SQLBACK.CMD
NET STOP MSSQLServer
```

Tämäkin voitaisiin vaikkapa ajastaa **AT**-komennolla.

NET TIME

Näyttää tai asettaa työaseman kellon samaan aikaan palvelimen kellon kanssa. Toimii myös LAN Manager-, Työryhmä-Windows- ja Windows 95-työasemissa. Windows NT-työasemassa kirjautuneella käyttäjätunnuksella tulee olla oikeus muuttaa NT-työaseman päiväystä ja kellonaikaa! Tätä oikeutta ei ole **Käyttäjät** (Users)-ryhmän jäsenillä!

Syntaksi:

NET TIME [\\MIKRO | /DOMAIN[:NIMI]] [/SET [/YES]]

Parametrit:

\\MIKRO	Tietokone, jonka aikaa käytetään
/DOMAIN[:NIMI]	Toimialue, jonka aikaa käytetään. Tätä parametria käytetään vain NT-tietokoneissa, jotka kuuluvat NT-toimialueeseen ja joihin ei ole asennettu NT Server -ohjelmistoa. Oletusarvona NT Server -tietokoneet suorittavat toiminnot toimialueen PDC:ssä
/SET	Asettaa tietokoneen kellon samaan aikaan määritetyn tietokoneen tai toimialueen kanssa
/YES	Automaattinen asetus

Esimerkki:

NET TIME /DOMAIN:HALLINTO /SET /Y

Asettaa automaattisesti työaseman/palvelimen ajaksi toimialueen **HALLINTO** PDC:n päiväyksen.

Kirjauskomentojonossa voidaan myös käyttää hyväksi **%USERDOMAIN%**-ympäristömuuttujaa:
NET TIME /DOMAIN:%USERDOMAIN% /SET /Y

NET USE

Luo tai katkaisee yhteyden palvelimesta tai työasemasta palvelimen tai työaseman jaettuun resurssiin tai näyttää tietoja työaseman verkkoyhteyksistä. Komennolla hallitaan myös **pysyviä** (*Persistent*) verkkoyhteyksiä.

Syntaksi:

NET USE [LAITENIMI] [\\PALVELIN\JAKONIMI [SALASANA| *]] [/USER:[TOIMIALUENIMI\]KÄYTTÄJÄ] [[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE LAITENIMI[/HOME[SALASANA | *]] [/PERSISTENT:{YES | NO}]

NET USE [/PERSISTENT:{YES | NO}]

Parametrit:

ei mitään	Näyttää verkkoyhteysluettelon
LAITENIMI	Muodostettavalle verkkoyhteydelle annettava nimi tai yhteys, joka katkaistaan. Laitenimiä on kahdenlaisia: levyasemia (D: - Z:) ja kirjoittimia (LPT1: - LPT3:)
\\PALVELIN\JAKONIMI	Palvelimen ja jaetun resurssin nimi. Jos palvelimen nimessä on välilyöntejä tai varattuja merkkejä, esimerkiksi &-merkki, tämä on kirjoitettava "lainausmerkkeihin"
SALASANA	Jaetun resurssin käyttöön tarvittava salasana
*	Salasana pyydetään kehotteella. Kehotteen perään kirjoitettu salasana ei näy näytössä
/USER	Käyttäjätunnus, jota käytetään yhteyttä muodostettaessa

TOIMIALUENIMI Määrittää toimialueen, jota käytetään yhteyttä muodostettaessa. Jos toimialuetta ei ole määritetty, käytetään toimialuetta, jolle käyttäjä on kirjautunut

KÄYTTÄJÄ Määrittää käyttäjätunnuksen, jota käytetään kirjauduttaessa

/HOME Yhdistää automaattisesti käyttäjän käyttäjälle määritettyyn kotihakemistoon

/DELETE Katkaisee annetun verkkoyhteyden

/PERSISTENT Määrittää, ovatko yhteydet pysyviä; oletusarvo on viimeksi käytössä ollut asetus. Yhteydet, joita ei ole kytketty laitenimeen, eivät voi olla pysyviä

yes Tallentaa yhteydet niiden muodostamisen yhteydessä ja palauttaa ne kirjauduttaessa seuraavan kerran

no Ei tallenna muodostettavaa yhteyttä eikä sen jälkeen luotavia yhteyksiä. Aiemmat yhteydet palautetaan kuitenkin seuraavan kirjautumisen yhteydessä. Pysyvät yhteydet poistetaan **/DELETE**-valitsimella

Esimerkkejä:

Testataan, onko hallinnoinnissa käytettävä nimetty putki riittävine oikeuksineen käytettävissä: **NET USE \\SPECTRE2\IPC$**

Otetaan käyttöön käyttäjätunnuksella **ADMIN** palvelimelta **SPECTRE5** jaettu hakemisto **DATA** levyasematunnukselle **X:** siten, että yhteys näyttää olevan luotu toimialueelta **HALLINTO** käyttäjätunnuksella **Pertti**:

NET USE X: \\SPECTRE5\DATA /USER:HALLINTO\PERTTI

Otetaan kirjoittimeksi **LPT3** palvelimen **V1** jakama kirjoitinjono **HP5Si**:

NET USE LPT3 \\V1\HP5SI

Tarkastellaan käyttöönotettua tulostusjonoa: **NET USE LPT3:**
Katkaistaan yhteys kirjoittimeen LPT3: **NET USE LPT3 /D**
Lopuksi katkaistaan kaikki verkkoyhteydet: **NET USE * /D**

Kaikkien verkkoyhteyksien katkaisemista kannattaa kokeilla, jos esimerkiksi työaseman työryhmän/toimialueen muuttaminen ei onnistu.

NET VIEW

Tuo näyttöön palvelinluettelon tai näyttää palvelimen jakamat resurssit.

Syntaksi:

NET VIEW [\\PALVELIN | /DOMAIN[:TOIMIALUE]]
NET VIEW /NETWORK:NW [\\PALVELIN]

Parametrit:

ei mitään Lista nykyisen toimialueen palvelimista

\\PALVELIN Palvelin, jonka jaettuja resursseja haluat tarkastella

/DOMAIN[:TOIMIALUE] Toimialue, jonka palvelinluettelon haluat näyttöön. Jos toimialuenimeä ei ole määritetty, luetteloon tulevat verkon kaikkien toimialueiden palvelimet

/NETWORK:NW NetWare-verkon palvelimet.

Esimerkkejä:

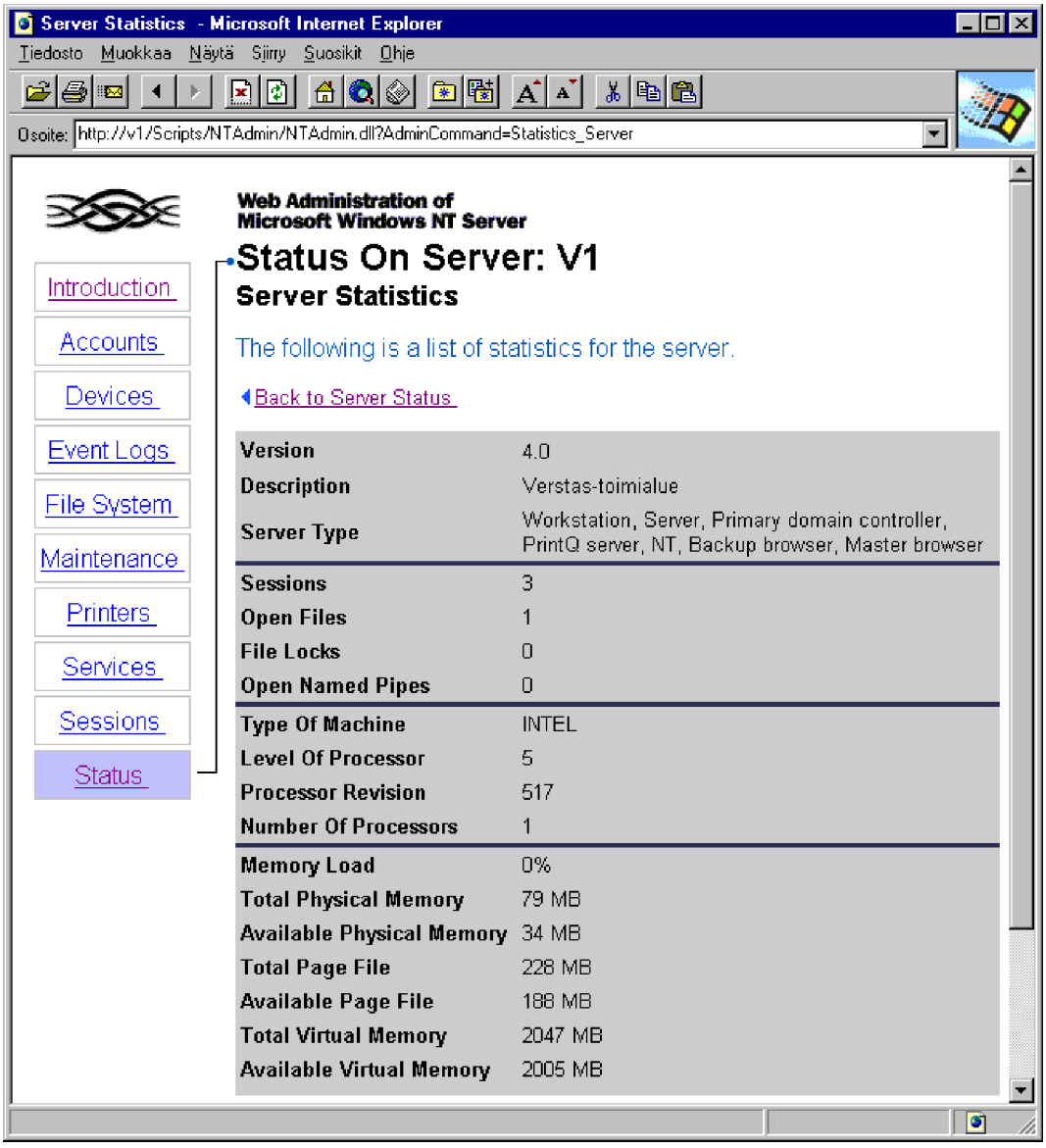
Halutaan selauspalvelun luettelo verkon toimialueen työasemista ja palvelimista: **NET VIEW**

Halutaan palvelimen **V1** jakamien resurssien lista ohittaen selauspalvelu:
NET VIEW \\V1

Palvelimen hallinta WWW-selaimella

Windows NT 4.0 Server Resource Kitin mukana tulee **Web Administration**-sovellus, joka on tarkoitettu IIS:ää ajavan NT 4.0-palvelimen hallintaan WWW-selaimella.

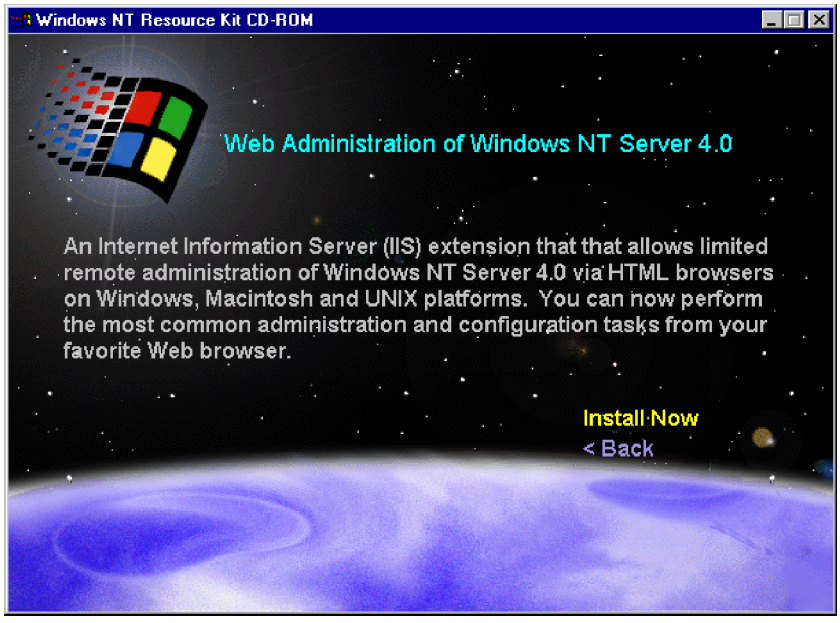
Jos tunnet NT-palvelimen hallintaperiaatteet niin tulet toimeen tämänkin hallintamenetelmän kanssa.



Käyttöönotto tehdään seuraavasti:

1) Ensin on asennettava palvelimeen Internet Information Server tavallisella asennusmenettelyllä. Asennus ei eroa WWW-vertaispalvelujen asennuksesta (ks. Luku 13). Valitse päävalikosta **Web Administration**

2) Asennetaan **Web Administration**-ohjelmisto **Windows NT 4.0 Server Resource Kitistä** valinnalla **Install Now**. (Uusin versio **Windows NT 4.0 Server Resource Kitistä** on kesäkuussa 1997 **Supplement 1**.)

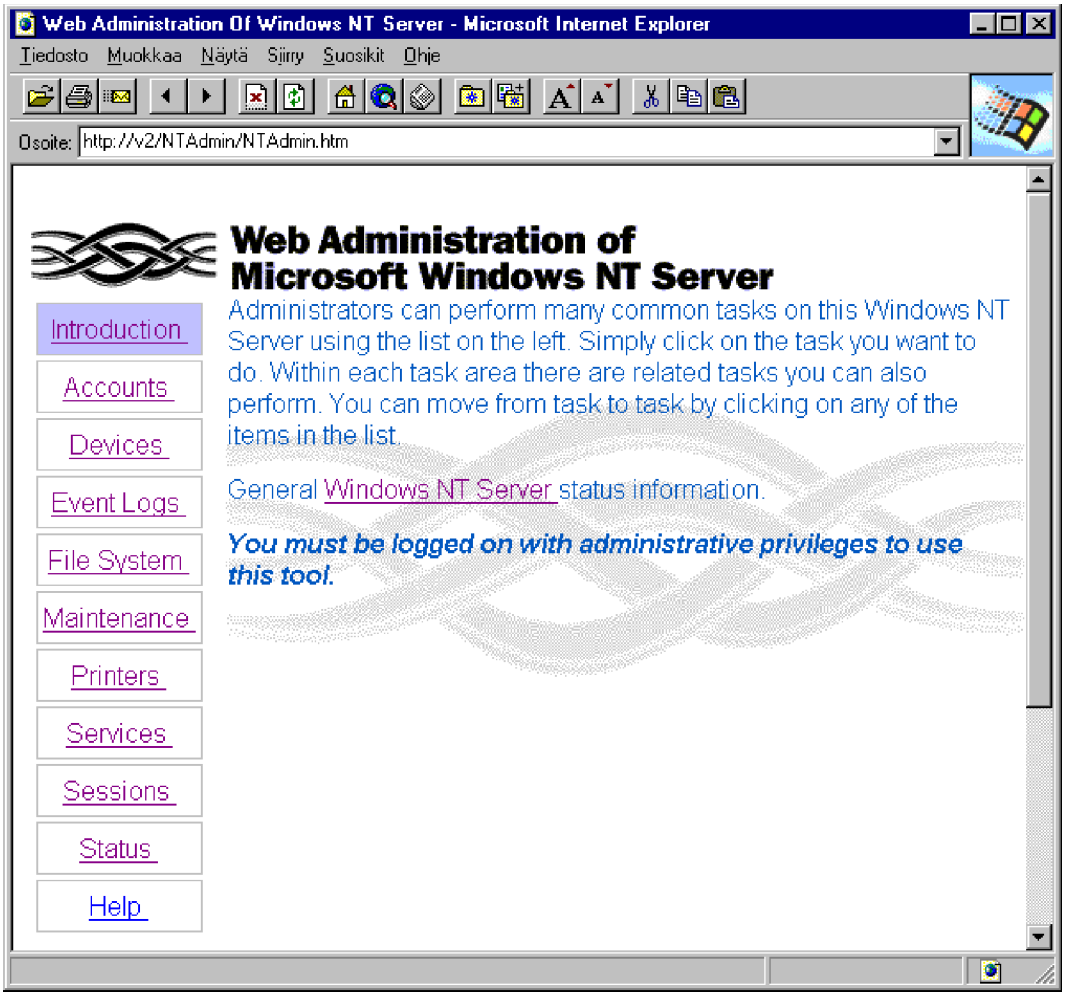


3) Asennus ei edellytä palvelimen uudelleenkäynnistystä. Asennuksen päätyttyä voit testata **ensin** palvelimen Internet Explorerilla kytkeytymistä palvelimen hallintaan; anna **Osoitteeksi** (Address)

localhost/ntadmin/ntadmin.htm

Tämän jälkeen voit työasemasta hallita NT-palvelinta. Osoite on

palvelin/ntadmin/ntadmin.htm



Jos et pääse kytkeytymään palvelimeen, tarkista:

- **Käyttöoikeustasosi** (Järjestelmänvalvoja (Administrator))
- **Nimiselvitysmenetelmä** (ks. Verkko, luku 11) ja TCP/IP-asetukset komennolla **IPCONFIG /ALL**:
  - Solmun tyyppi
  - WINS/DNS-asetukset
  - Isäntätiedostot (LMHOSTS, HOSTS)
- Palvelimen tilanne (status).

Päävalikon valinnat ovat:

- **Introduction** - yleinen palvelimen tilanne
- **Accounts** - käyttäjätunnusten, ryhmien ja toimialueen tietokoneiden tilien (konetunnusten) hallinta
- **Devices** - laiteohjainten hallinta
- **Event Logs** - tapahtumalokit
- **File System** - jaettujen resurssien ja kansioiden sekä tiedostojen käyttöoikeudet
- **Maintenance** - sanomien lähetys (**Broadcast**) palvelimeen kytketyneille käyttäjille, palvelimen uudelleenkäynnistys **(Reboot)**, konsolin etähallinta (**Remote Console**, edellyttää palvelimeen asennettua Remote Console-tukea) ja WWW-hallintaohjelman oletusasetukset
- **Printers** - kirjoittimien hallinta
- **Services** - palveluiden hallinta
- **Sessions** - istuntojen hallinta
- **Status** - palvelimen palveluiden asetukset (**Server Configuration**), suorituskyvyn tilastotiedot (**Performance Statistics**) ja palvelimen tilastotiedot (**Server Statistics**)
- **Help** - opaste, mm. lista tuetuista WWW-selaimista.

Verkkoasemat

Verkkoresursseja voit hallita seuraavilla menetelmillä:

- Resurssienhallinta (Explorer)
- My Computer
- Network Neighbourhood
- Server Manager
- File Manager, joka pitää erikseen käynnistää **WINFILE**-komennolla. File Manager tarjoaa edelleenkin joitakin verkkoresurssien hallinnan ominaisuuksia, jotka Windows NT 4.0:n käyttöliittymästä puuttuvat.

Verkkoresursseja on käsitelty perusteellisesti **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

Suojauksia ja **valvontaa** on käsitelty luvussa **11**.

Seuraavaksi käsitellään lyhyesti keskeiset periaatteet.

Kansion jakaminen

Kansion jakaminen tehdään valitsemalla haluttu kohde ja antamalla sen käyttöoikeudet:

- Palvelinpalvelun (Server) on oltava käynnissä, ennen kuin voit jakaa kansioita

- Jotta voisit jakaa kansion, sinun on kirjauduttava **Administrators**-, **Server Operators**- tai **Power Users**-ryhmän jäsenenä

Kansion jakaminen tehdään resurssienhallinnalla (Explorer) seuraavasti:

1) Valitse **My Computer**.

2) Valinnalla näet kyseisen NT -palvelimen resurssit. Voit jakaa palvelimen kiintolevyjen, CD-ROM-asemien, siirrettävien kiintolevyjen (esimerkiksi Iomega) ja levykeasemien kansioita. Jos jaettava kansio on D:-asemassa, kaksoisnapautetaan D:-aseman kuvakkeen päällä, jolloin saadaan ikkuna D:-aseman kansioista

3) Painetaan hiiren oikeanpuolista painiketta, jolloin voidaan valita **Sharing**

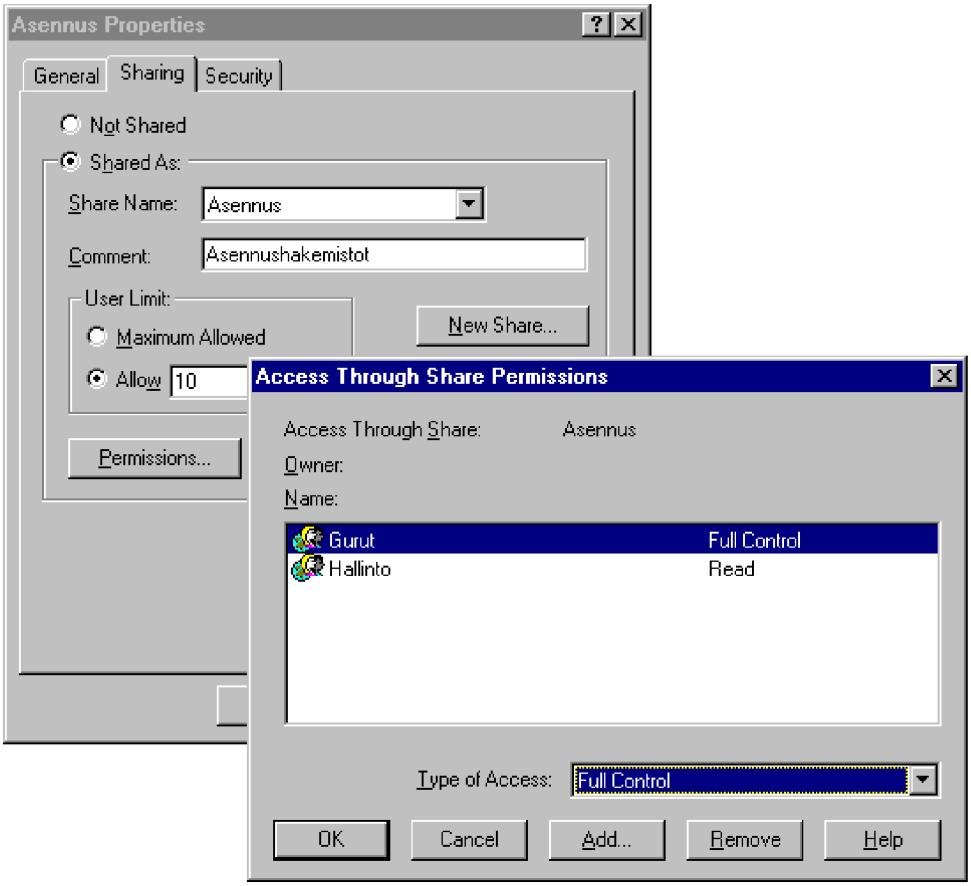
4) Anna jakamisen asetukset:

- **Not Shared** ilmaisee, että resurssi ei ole jaettu
- **Shared As** -valinnalla voidaan antaa jaon asetukset
- **New Share** - voit jakaa jo jaetun kansion uudella nimellä, uusilla oikeuksilla ja uudella kuvauksilla
- **Share Name** on jakonimi. Anna se siten kuin haluat sen verkossa näkyvän. Oletuksena tähän tulee kansion kiintolevyllä oleva nimi. Jakonimi saa olla 12 merkkiä pitkä ja siinä saa olla kirjaimia, numeroita ja jopa merkit !#$%()-.@ ^ _'{}~. Jos lisäät kansion viimeiseksi merkiksi **$**-merkin, se ei näy työasemasi jakamien kansioiden listassa vaan siitä tulee **piilotettu jakonimi**
- **Comment** tulee näkyviin, kun käyttäjä selaa jaettuja resursseja - kommenttia ei ole pakko kirjoittaa
- **User Limit** -käyttäjärajoituksen **Allow**-ruudussa voit määritellä moniko käyttäjä voi käyttää jaettua kansioita samanaikaisesti. Oletusarvo on, että määrää ei ole rajoitettu eli **Maximum Allowed**

5) Määritä jaetun kansion käyttöoikeudet verkon kautta valitsemalla **Permissions**-painike. Voit määrittää seuraavat käyttöoikeudet jaetulle resurssille **Access Through Share Permissions**, pienimmästä suurimpaan:

- **Read** - lukuoikeus
- **Change** - muutosoikeudet
- **Full Control** - täydet oikeudet
- **No Access** - ei käyttöoikeutta

Muista, että oikeudet kumuloituvat - jos käyttäjällä on esimerkiksi eri ryhmien kautta erilaisia oikeuksia, hänen käytössä olevat oikeutensa ovat näistä suurimmat. **No Access** kuitenkin ohittaa kaiken muun. Käyttöoikeudet koskevat myös kaikkia jaetun kansion alikansioita. Jaetun kansion käyttöoikeuksien poistaminen tehdään valitsemalla ryhmän tai käyttäjän nimi ja painamalla **Remove**.



6) Paina lopuksi **OK** ja kansio on jaettu verkkoon - jaetun kansion huomaat kädestä, joka ikäänkuin ojentaa kansiota.

Huomaa:

- Voit myös hallita jaettuja kansioita **NET SHARE** -komennolla sekä **Server Manager**-ohjelmalla!

- Pyri jakamaan kansiot NTFS-levyltä ja käytät hyväksesi NTFS:n mahdollistamia suojauksia! Katso suojauksia käsittelevä luku **11**.

Kansion jaon lopettaminen

Jakaminen lopetetaan valitsemalla kansio ja painamalla hiiren oikeanpuoleista painiketta, jolloin voidaan valita **Sharing**-valinnasta **Not Shared**.

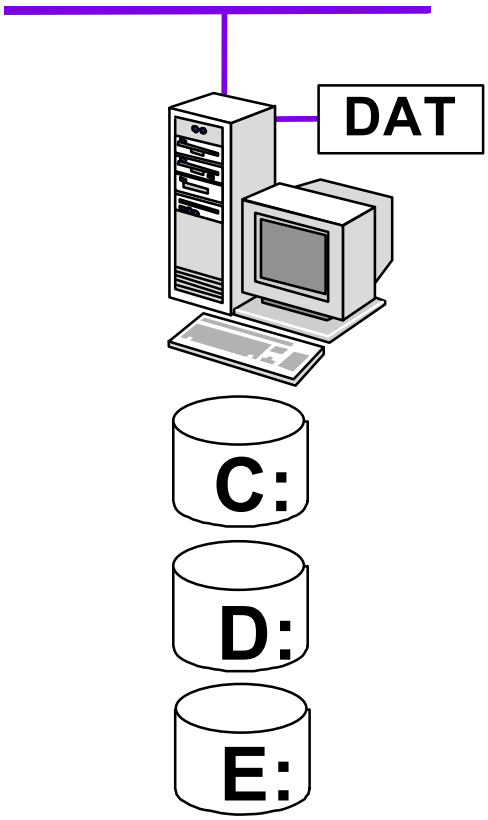
Windows NT luo automaattisesti tietyt jakonimet **järjestelmäkäyttöä** varten. Kun palvelinpalvelu käynnistetään, luodaan automaattisesti jakonimet **jokaiselle juurihakemistolle** sekä NT:n **järjestelmän päähakemistolle** (esimerkiksi C:\WINNT-hakemisto). Järjestelmä nimeää nämä hakemistot käyttämällä aseman tunnusta ja $-merkkiä, esimerkiksi C$. Järjestelmän päähakemistoa varten luodun jaetun hakemiston nimi on **ADMIN$**. Lisäksi jaetaan esimerkiksi **PRINT$** (kirjoitin) ja **IPC$** (nimetyt putket) sekä palvelimessa **REPL$** (monistuspalvelu) ja **NETLOGON$** (kirjautumiskomentojonot eli logon scriptit). Älä poista näiden resurssien jakamista ilman erityistä syytä!

Kansiohierarkia

Kansiohierarkia eli hakemistorakenne kannattaa suunnitella palvelimen levyosioilla huomioiden seuraavat seikat:

- Yksinkertaisuus (rakenne on muidenkin pääkäyttäjien ymmärrettävissä)
- Varmistusmenetelmä on mahdollinen, esimerkiksi kokonaisen levyosion varmistus ja palautus yhdellä kerralla
- Suojaukset ovat käytössä ja hyödynnetty mahdollisimman tehokkaasti (NTFS, hakemistorakenne, eri levyosiot)
- Käyttöjärjestelmän vaatimukset on huomioitu (sivutustiedoston koko ja sijainti, tulostusjonot).

Seuraava esimerkki pyrkii kuvaamaan tyypillisen **tiedosto- ja tulostuspalvelimen** hakemistorakennetta. Levyosiot ovat **C:**, **D:** ja **E:** riippumatta siitä, ovatko ne erillisiä kiintolevyjä vai onko palvelimessa RAID-levyjärjestelmä. Palvelimessa on lisäksi **Internet Information Server**. Kansiohierarkian periaatteena ovat olleet edellä esitetyt seikat:



Levyasemat hakemistoineen ovat seuraavat:

Levyasema	Hakemisto	Hakemiston kuvaus
C:	\	**Windows NT:n järjestelmälevy**. Hakemisto Winnt on NT:n järjestelmähakemisto. Levyllä on lisäksi kooltaan RAM + 12 Mt sivutustiedosto (pagefile.sys). Levyn koko on 300 - 500 Mt, vapaata levytilaa tulisi olla 100 Mt
C:	ADMIN$	Hakemisto Winnt on NT:n järjestelmähakemisto
C:	NETLOGON	Kirjauskomentojonot, Default User-kansio, NTConfig.pol
C:	PRINT$	Kirjoittimien käsittely, kirjoitinohjaimet
C:	REPL$	Monistuspalvelu
D:	\	Levyllä on sivutustiedosto (pagefile.sys).

D:	Data	**Käyttäjien datatiedostoja**, verkon kautta tarpeellisille käyttäjäryhmille Full Control tai Change, NTFS-oikeudet hakemistoilla asetettu käyttäjäryhmäkohtaisesti
D:	Profiles	Profiilien hakemistot, NTFS-oikeudet alihakemistoilla asetettu käyttäjäkohtaisesti
D:	Apps	Sovellusten hakemistot, verkon kautta tarpeellisille käyttäjäryhmille Full Control tai Read, NTFS-tasolla käyttäjillä lukuoikeus Read, järjestelmänvalvojilla oikeudet tarpeen mukaan
D:	Asennus	Sovellusten asennushakemistot, verkon kautta vain järjestelmänvalvojilla **Full Control**, samoin NTFS-tasolla
D:	Users	Käyttäjien kotihakemistoja, verkon kautta tarpeellisille käyttäjäryhmille Full Control, päähakemistossa NTFS-tasolla luetteluoikeus **List**, alihakemistoilla oikeudet asetettu **Full Control** käyttäjäkohtaisesti
E:	\	Levyllä on sivutustiedosto (pagefile.sys).
E:	InetPub	**IIS:n päähakemisto**, alihakemistoissa ftproot, gophroot, scripts, wwwroot, NTFS-tasolla käyttäjillä pääasiassa lukuoikeus Read, järjestelmänvalvojilla oikeudet tarpeen mukaan
E:	Printers	Kirjoittimien tulostusjonot (voi sijaita D:lläkin)

Huomattavaa:

- Varmistamalla paikallisella varmistusnauhurilla (DAT- tai DLT-tyyppinen) rekisteri, D:- ja E:-levyasemat saadaan järjestelmän ja käyttäjien kannalta oleelliset tiedostot talteen. Varmistuksen ajastus hoidetaan AT-komennolla ja Schedule-palvelulla

- Varmistus voidaan hoitaa myös verkon yli, mutta NT:n oma Backup-ohjelma ei tue rekisterin varmistusta verkon yli

- Sivutustiedosto on jaettu useammalle levylle siitä syystä, että jos yksi (tai kaksikin) levyasema tulee täyteen, sivutustiedosto voi tarvittaessa kasvaa kolmannella levyllä

- Kirjoittimien tulostusjonot on ohjattu NT:n systeemilevyltä E:-levylle. Syynä tässä esimerkin ratkaisussa voisi olla se, että E: ei ole yhtä kuormitettu kuin D:-levy.

Verkkokirjoittimet

Kirjoittimia hallitaan **Printers**-kansion sekä **Network Neighborhood**in avulla. Kirjoittimien asetuksia on käsitelty luvussa **3**.

Verkkokirjoittimen perusteita on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

Kirjoitinohjaimet

Kirjoittimen käytössä tarvitaan a.o. kirjoittimen **kirjoitinohjain** (*Printer Driver* eli kirjoitinajuri). Arkkitehtuurimuutoksen johdosta Windows NT 4.0 vaatii **Windows NT 4.0-version kirjoitinohjaimesta**! Windows NT 3.51-versio **ei** käy. Ei myöskään Windows 95-versio. Yhteiset kirjoitinohjaimet tulevat vasta Windows NT 5.0:n ja *Memphisin* myötä.

Koska kuitenkin Windows 95- ja Windows NT-verkoissa kirjoitinta jakava palvelin voi palauttaa kirjoittimeen kytkeytyvälle työasemalle kirjoitinohjaimet, tulostus Windows 95-työasemalta Windows NT 3.51-palvelimelle vaatii Windows 95-työasemassa asennetun paikallisen kirjoitinohjaimen. Samoin Työryhmä-Windows (Windows for Workgroups) vaatii asennetun paikallisen kirjoitinohjaimen.

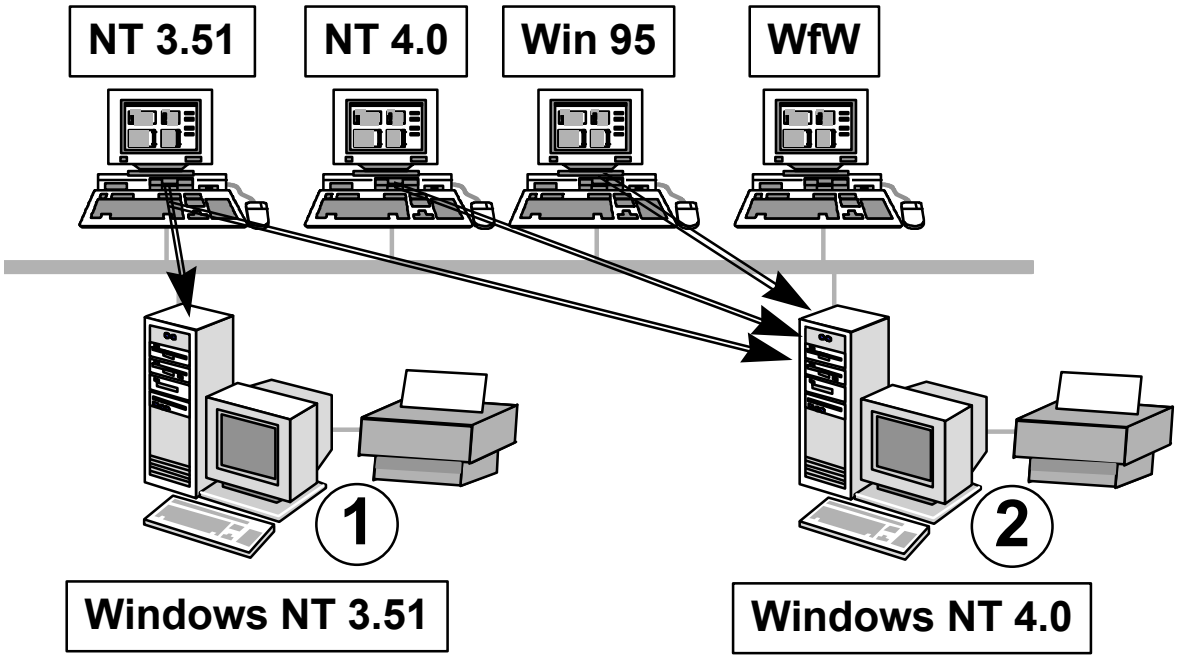
Uusi piirre Windows NT 4.0:ssa on se, että Windows NT 4.0-palvelin voi jakaa kirjoitinohjaimia Windows 95- ja Windows NT 3.51-työasemille, mutta edelleen Työryhmä-Windows (Windows for Workgroups) vaatii kyseiseen työasemaan asennetun paikallisen kirjoitinohjaimen.

Tilannetta kuvaavat seuraavan piirroksen nuolet. Nuoli tarkoittaa

tulostamista palvelimen jakamalle kirjoittimelle ilman ennalta asennettua paikallista kirjoitinohjainta:

- Windows NT 3.51-palvelimelle (**1**) voi tulostaa ilman ennalta asennettua paikallista kirjoitinohjainta vain Windows NT 3.51-työasema. Muut työasemat vaativat paikallisen kirjoitinohjaimen asentamisen.

- Windows NT 4.0-palvelin (**2**) voi jakaa kirjoitinohjaimia Windows 95-, Windows NT 4.0- ja Windows NT 3.51-työasemille, mutta edelleen Työryhmä-Windows (Windows for Workgroups) vaatii kyseiseen työasemaan asennetun paikallisen kirjoitinohjaimen. Lisäksi Työryhmä-Windows (Windows for Workgroups) kytkeytyy LPT-tunnuksella kirjoittimeen, UNC-nimiä ei voi käyttää.



Jos kirjoitin on asennettu Windows NT-koneeseen, mutta **ei** jaettu, sen voi silti selata verkon kautta **Network Neighborhoodin** avulla. Jos jakamattomat kirjoittimet halutaan piilottaa, eräs ratkaisu on käyttää **Policy Editoria**, jossa voidaan kirjoittimien kohdalla antaa valinta **Disable Browse Thread**.

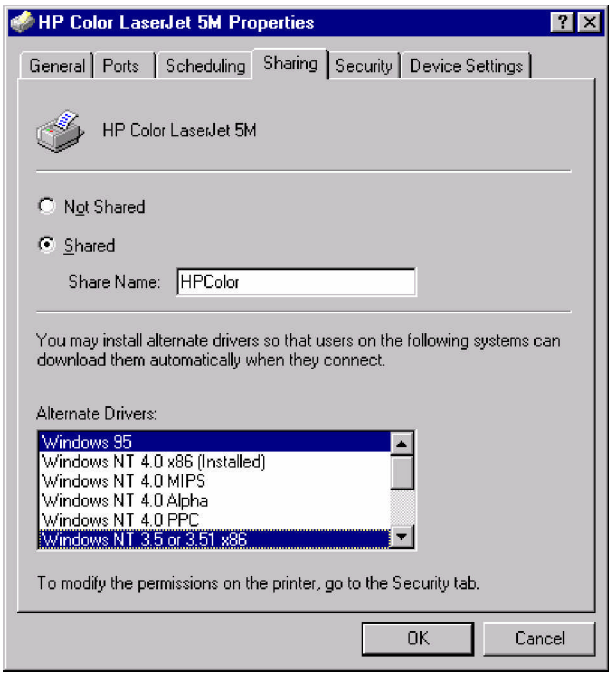
Verkkokirjoittimen jakaminen

Paikallisen kirjoittimen jakaminen tehdään valitsemalla haluttu kirjoitin ja antamalla sen jakomääritykset. Toinen tapa jakaa kirjoitinta on jakaa se jo asennuksen yhteydessä **Add Printer Wizard**illa.

Olemassaolevan kirjoittimen jakaminen tehdään seuraavasti:

1) Avaa **Printers** -kansio. Valitse jaettava kirjoitin ja valitse **File | Sharing** tai paina hiiren oikeanpuoleista painiketta, jolloin voit valita **Sharing**.

2) Anna jakamisen asetukset **Sharing**-välilehdessä. **Not Shared** ilmaisee, että resurssi ei ole jaettu. Valitaan **Shared** ja annetaan **Shared Name**-kohtaan jakonimi. Anna kirjoittimen verkossa käytettävä nimi; samalla voit valita **kirjoitinohjaimet** eri käyttöjärjestelmille. Tällöin tarvitset myös a.o. käyttöjärjestelmien kirjoitinajurit!



3) **Security**-välilehden **Permissions**-painikkeella voidaan antaa käyttäjille oikeuksia kyseiseen resurssiin. Oletuksena **Everyone**-ryhmällä on tulostusoikeudet (**Print**) ja tulostustyön luoja (**Creator-Owner**) voi hallita täysin omaa tulostustyötään. Oikeudet **Type of**

Access-listassa ovat seuraavat:

- **No Access** - kirjoittimelle ei voi tulosta eikä kirjoitinta ei voi hallita
- **Print** - tulostaminen ja omistettujen tulostustöiden hallinnointi on mahdollista
- **Manage Documents** - kaikki **Print**-oikeudet sekä tulostusjonossa olevien töiden hallinta
- **Full Control** - kaikki **Manage Documents**-oikeudet sekä kirjoittimien jakaminen, ominaisuuksien muuttaminen, kirjoittimen poistaminen ja kirjoittimen käyttöoikeuksien muuttaminen.

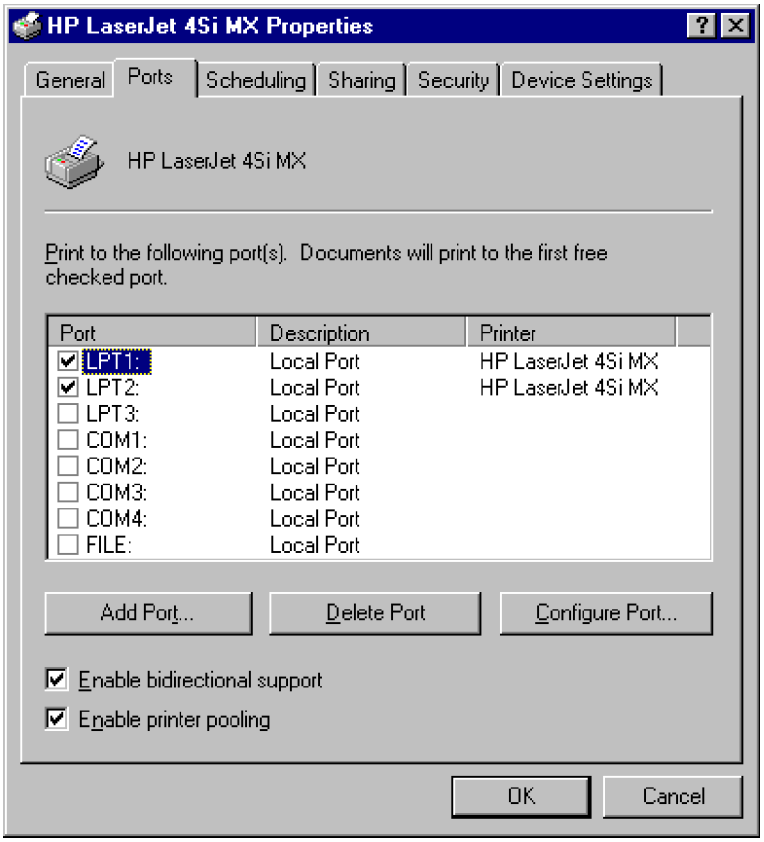
4) Paina lopuksi **OK**. Kirjoitin on jaettu verkkoon. Sen huomaat kädestä, joka ojentaa kirjoitinta.

Muita asetuksia:

- Kommentin (**Comment**) voit lisätä **General**-välilehdessä
- **Ports**-välilehdessä voit määritellä kirjoitinvarannon (**Enable Printer Pooling**), eli useamman portin, joissa on samanlainen kirjoitin, ja jotka jakavat tulostustyöt ja kaksisuuntaisen portin tuen (**Bidirectional support**)
- **Scheduling**-välilehdessä voit määritellä tulostusajan
- **Device Settings**-välilehdessä voit määritellä laitekohtaisia asetuksia, kuten muistin jne.

Kirjoitinvaranto

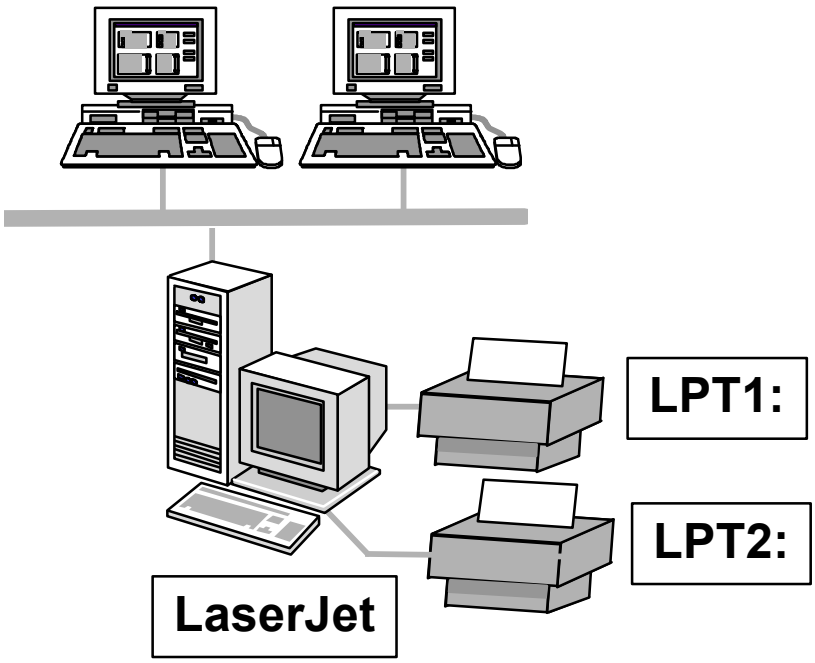
Ports-välilehdessä voit määritellä kirjoitinvarannon valinnalla **Enable Printer Pooling**, eli useamman portin, joissa on samanlainen kirjoitin, ja jotka jakavat kirjoittimelle ohjatut tulostustyöt.



Portti voi olla myös verkkoon liitetty kirjoitin. Etuja tällaisesta järjestelystä ovat seuraavat:

- Tulostustyö ohjataan ensimmäiselle vapaalle kirjoittimelle
- Jos paperi tai värijauhe loppuu, tulostus jatkuu toiselle kirjoittimelle (vain yksi työ jää odottamaan paperin tai värijauheen lisäämistä)
- Jos kirjoitin menee jumiin, vain yksi työ jää jumiin
- Tulostus toimii samanaikaisesti molemmilla kirjoittimilla
- Vanhoja kirjoittimia saadaan näin tehokäyttöön.

Tässä esimerkissä palvelin jakaa **LaserJet**-nimistä kirjoitinta, joka on kytketty rinnakkaisportteihin **LPT1:** ja **LPT2:**.



Käyttäjät kytkeytyvät palvelimen **LaserJet**-jakoon, ja palvelin hoitaa tulostuksen ohjauksen jommalle kummalle kirjoittimelle.

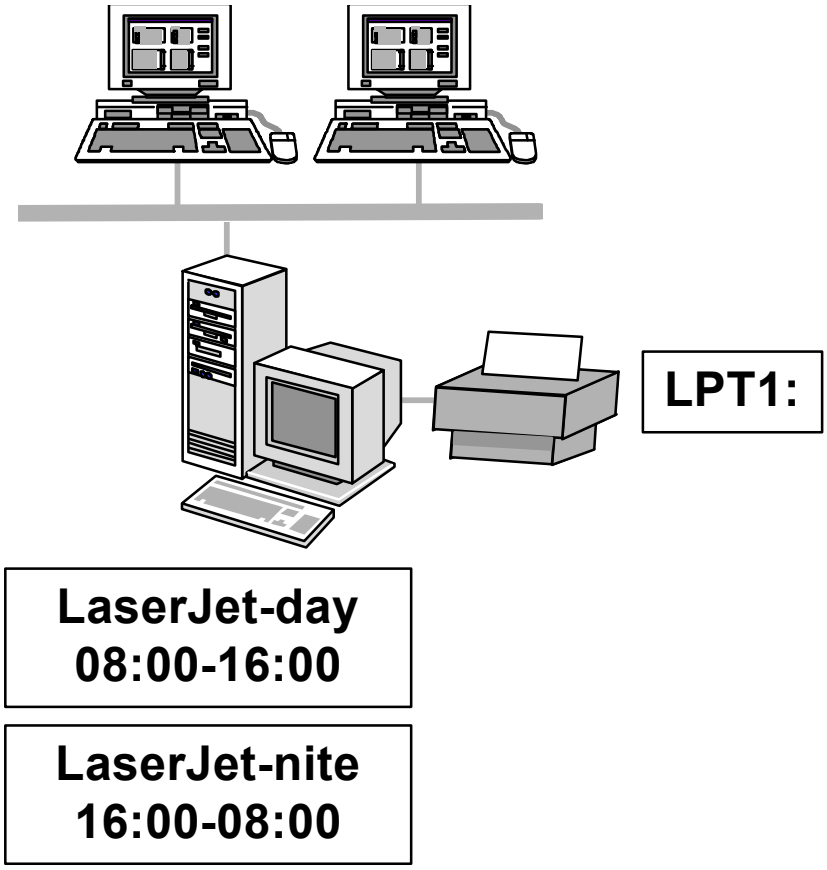
Kirjoittimien ajastaminen

Eräs mahdollisuus on asentaa useampi kirjoitinohjain ja määritellä kohteeksi sama kirjoitin (esimerkiksi LaserJet LPT1:-portissa). Kirjoittimien käyttöaika porrastetaan. Tällä saavutetaan seuraavia etuja:

- Voidaan ohjeistaa tulostamaan pitkät dokumentit, jotka eivät ole kiireellisiä, kirjoittimelle joka tulostaa ne illalla. Tulostukset menevät kirjoittimen tulostusjonoon, joka odottaa määriteltyä tulostusaikaa ja käynnistää tulostuksen **automaattisesti** halutuna aikana

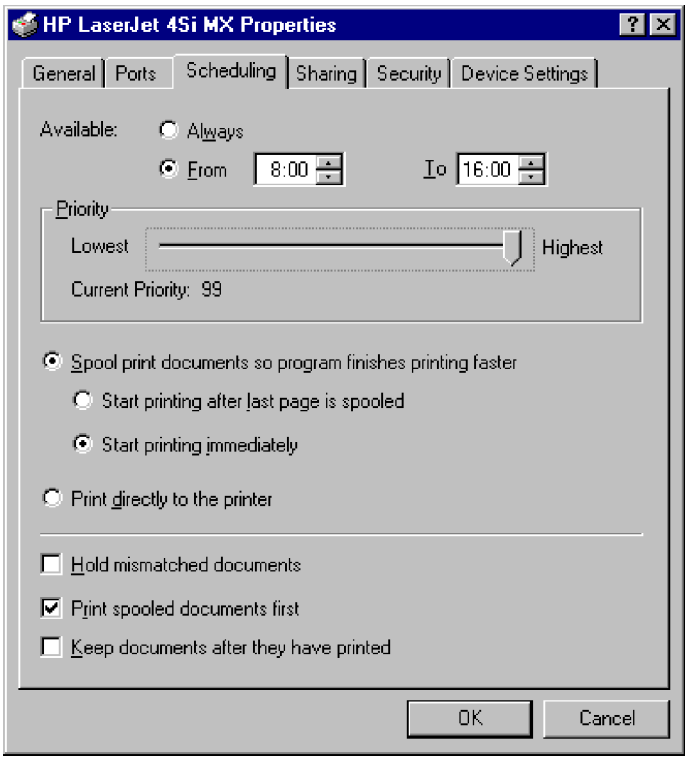
- Voidaan ohjeistaa tulostamaan heti tarvittavat dokumentit kirjoittimelle, joka tulostaa ne välittömästi.

Voidaan toki soveltaa myös kirjoitinvarantoa tässäkin tapauksessa.

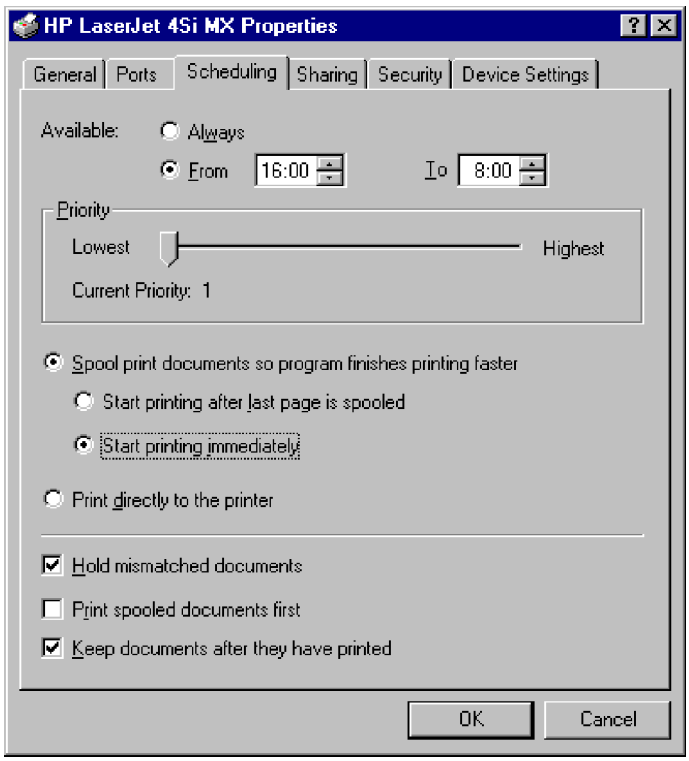


Esimerkissä on kaksi kirjoitinta, **LaserJet-day** ja **LaserJet-nite**, jotka tulostavat päivällä ja yöllä.

Asetuksissa kannattaa huomioida **Scheduling**-välilehdessä prioriteetti sekä tulostustöiden käsittely. Tässä on **LaserJet-day** -kirjoittimen asetukset:

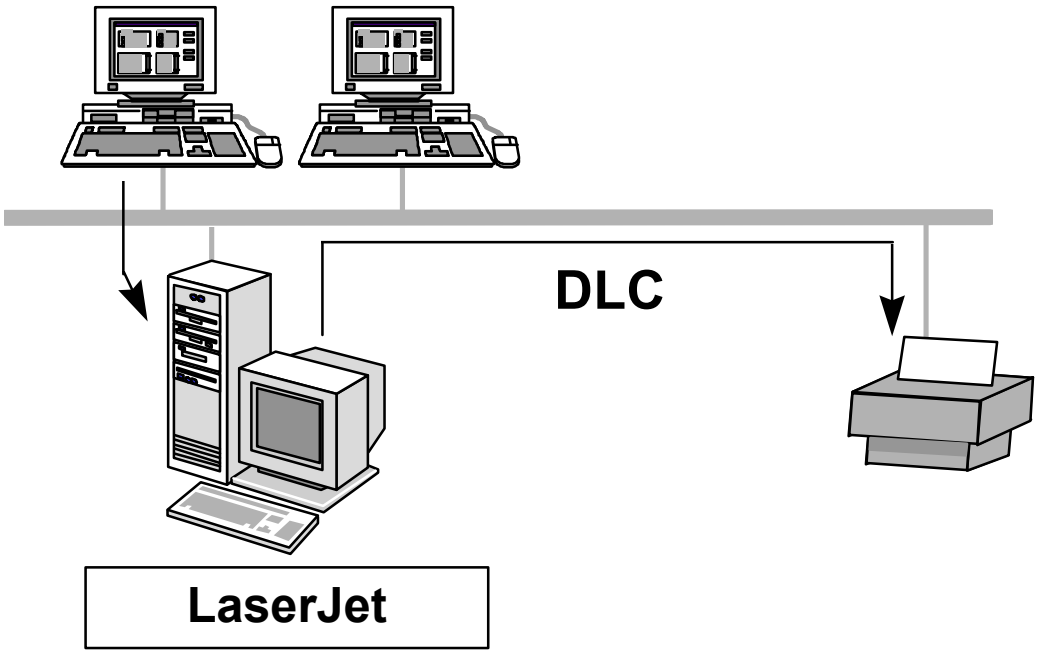


Ja tässä **LaserJet-nite** -kirjoittimen asetukset: huomaa, että tulostustyöt jätetään tulostusjonoon siltä varalta että tulostuksessa meni jotain pieleen. Tällöin tulostusta ei tarvitse tehdä uudelleen sovelluksesta.



Verkkoon liitetyn kirjoittimen jakaminen

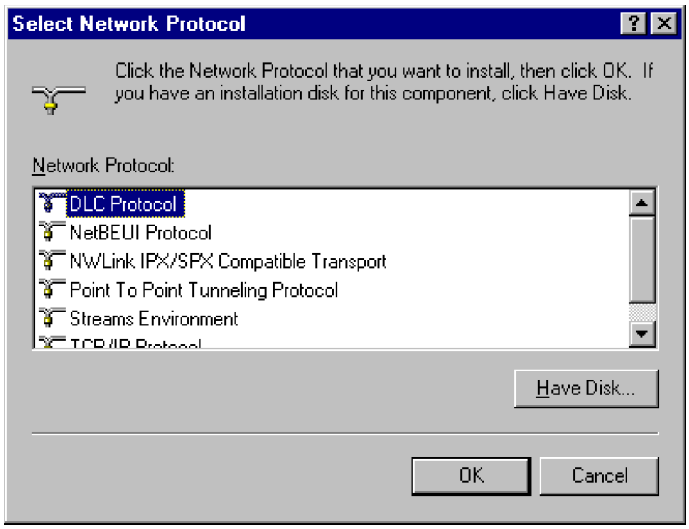
Voit jakaa NT-palvelimelta myös suoraan verkkoon liitetyn kirjoittimen. Tällöin kirjoittimessa on joko oma verkkoliitäntänsä tai käytetään esimerkiksi **HP JetDirect EX**-liitäntää. Käyttäjät kytkeytyvät NT-palvelimen jakamaan kirjoittimeen, ja palvelin ohjaa tulostuksen edelleen verkon kirjoittimelle.



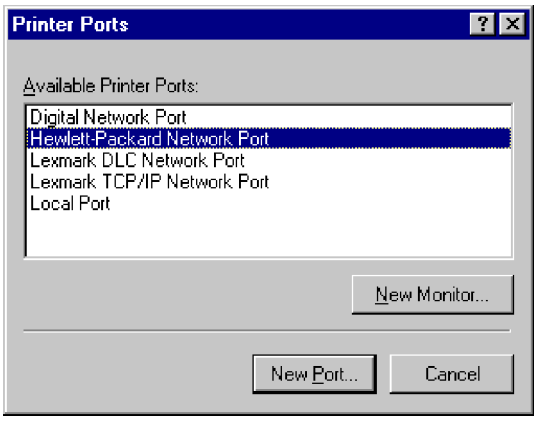
Palvelimen ja kirjoittimen on käytettävä yhteistä protokollaa. Tavallisesti tällainen protokolla on **DLC** tai **TCP/IP**. Työasemat ja palvelin vastaavasti käyttävät yhteistä protokollaa, vaikkapa **NetBEUI**, **IPX/SPX** tai **TCP/IP**.

Suoraan verkkoon liitetyn kirjoittimen jakaminen tehdään seuraavasti:

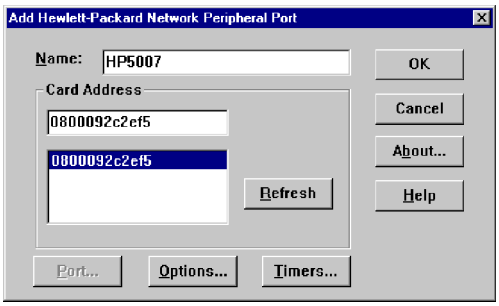
1) Asenna NT-palvelimeen tarvittava protokolla, esimerkiksi **DLC**. Käytä Ohjauspaneelin **Network**-kuvakkeen **Protocols**-valintaikkunaa. Käynnistä palvelin uudelleen



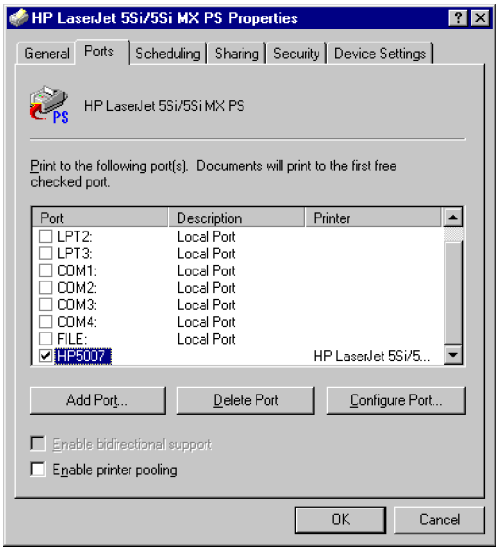
2) Lisätään haluttu portti. Jos haluamaasi porttia ei ole luettelossa, valitse **Add Port** ja valitse **Printer Ports** -valintaikkunasta haluttu kohde.



3) Valitse HP-kirjoittimen tapauksessa **Hewlett-Packard Network Port** ja paina **New Port**. **Card Address**-luetteloruudusta voit valita halutun kirjoittimen osoitteen. Anna portille nimi **Name**-kohtaan. Valitse tarvittaessa lisäasetukset **Port**-, **Options**- ja **Timers**-painikkeilla sekä valitse lopuksi **OK**



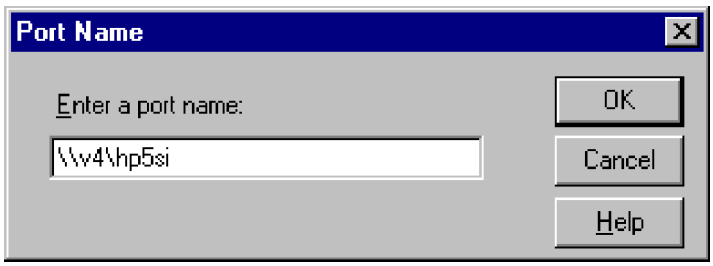
4) Verkkokirjoitin tulee porttien listaan. Tämän jälkeen voit konfiguroida kirjoittimen kuten paikallisenkin kirjoittimen tapauksessa.



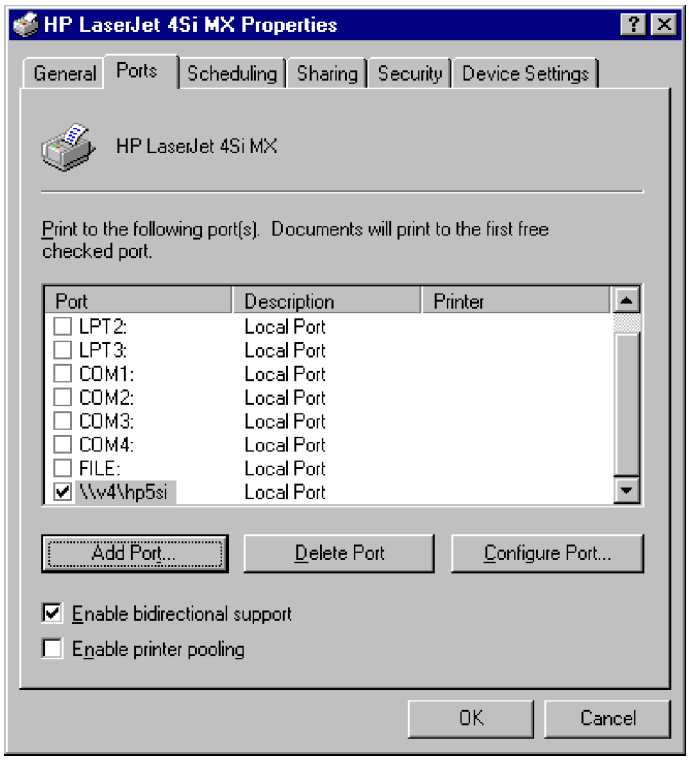
Voit poistaa portin painikkeella **Delete Port**.

Tulostuksen uudelleenohjaaminen

Voit ohjata tulostuksen toiseen NT-palvelimeen valitsemalla **Add Port** ja valitse **Printer Ports** -valintaikkunasta **Local Port**. Anna verkkokirjoittimen **UNC**-nimi:



Verkkokirjoitin tulee porttien listaan.



Kirjoitinpalvelin

Printers-kansion **File** | **Server Properties** määrittelee kaikki NT-mikron jakamille kirjoittimille yhteiset asetukset.

Valinta on käytettävissä myös, jos valitset **Network Neighborhood**- tai resurssienhallinta (Explorer)-ikkunoissa **Printers**-kansion. Voit tällöin määritellä myös verkon kautta kirjoitinpalvelimen asetukset.

Käytettävissä on kolme välilehteä: lomakkeiden asetukset (**Forms**), portit (**Ports**) ja lisäasetukset (**Advanced**).

Forms

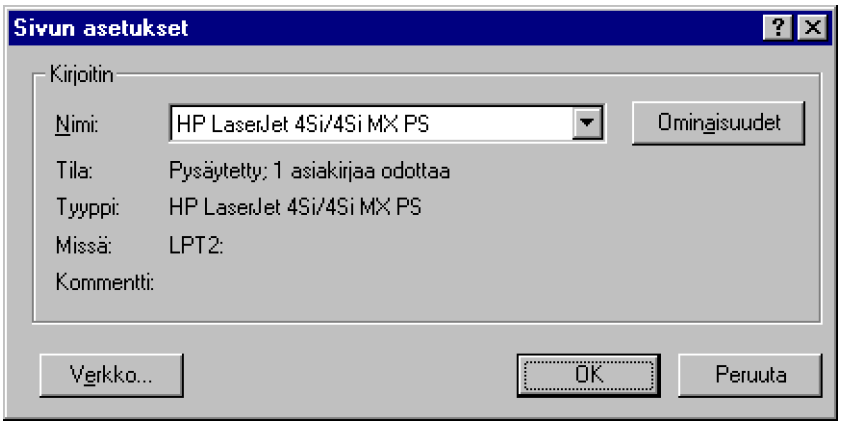
Forms-välilehti määrittää paperin ja sen reunuksien koon. Voit määrittää oman paperikoon kirjoittimen jokaiselle syöttölokerolle, esimerkiksi eri paperikoko ylä- ja alalokerolle. Standardikokojen lisäksi voit luoda omia paperikokoja ja määrittää kirjoittimen käyttämään niitä. Luo tietyssä kirjoittimessa käytettävä paperikoko kyseisen kirjoittimen palvelimessa seuraavasti:

1) Valitse olemassa oleva lomake

2) Tee esimerkiksi **Logo**-niminen A4-kokoinen paperikoko, jonka ylä- ja alareunus ovat normaalia leveämmät firman logoa varten; valitse ensin **A4** ja valitse **Create a New Form** - anna uusi nimi **Form Description for**-ruutuun; muuta asetus **Top** ja **Bottom** hieman suuremmaksi. Paina lopuksi **Save Form**

3) Määritä sen jälkeen tämä paperikoko jonkin kirjoittimen syöttölokerolle kyseisen kirjoittimen **Document Defaults**-oletuksista.

4) Kirjoittimen käyttäjät voivat valita Logo-paperikoon, kun he haluavat tulostaa sovelluksistaan logolomakkeille valitsemalla työasemissaan kirjoittimen **Ominaisuudet** (Properties).

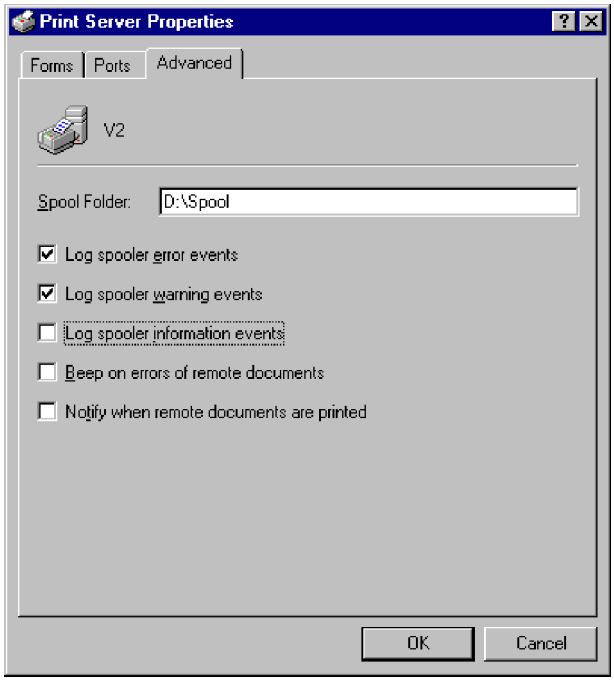


Ports

Ports-välilehdessä voit määritellä käytettävissä olevat kirjoitinportit. Voit poistaa portin painikkeella **Delete Port**. **Configure Port**-asetuksella voit asettaa aikakatkaisun eli ajan, jonka kuluttua NT päättää, että kirjoitin ei vastaa. Asetus vaikuttaa **kaikkiin samaa porttia** käyttäviin **paikallisiin kirjoittimiin**. Asetus **Transmission Retry** määrittää ajan, jonka Tulostuksenhallinta odottaa ennen seuraavaa tulostamisyritystä; anna aika sekunteina.

Advanced

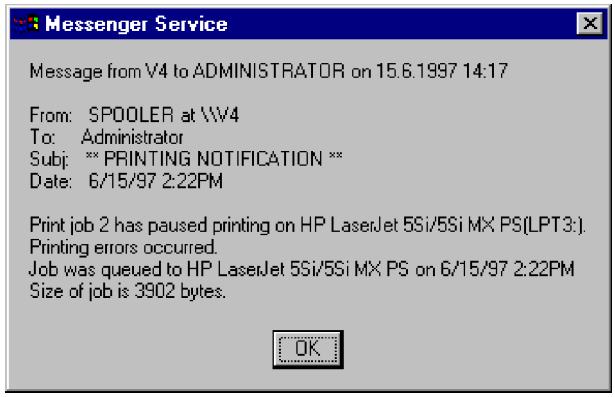
Advanced-asetuksista voit määritellä seuraavat asetukset:



- **Spool Folder** on hakemisto, johon tulostusjonon työt ohjataan. Esimerkiksi tilanteessa, jossa NT:n järjestelmälevy alkaa tulla täyteen, on syytä ohjata tulostusjonon työt toiseen levyasemaan! Esimerkissä se on **D:\Spool**

- **Log**-asetukset tallentavat ongelmatilanteet tapahtumalokiin

- **Notify when remote documents are printed** tuo näyttöön ilmoituksen tulostuksesta - tämä voidaan useimmiten jättää pois, jos näyttöön tulevat ilmoitukset aiheuttavat riesaa.



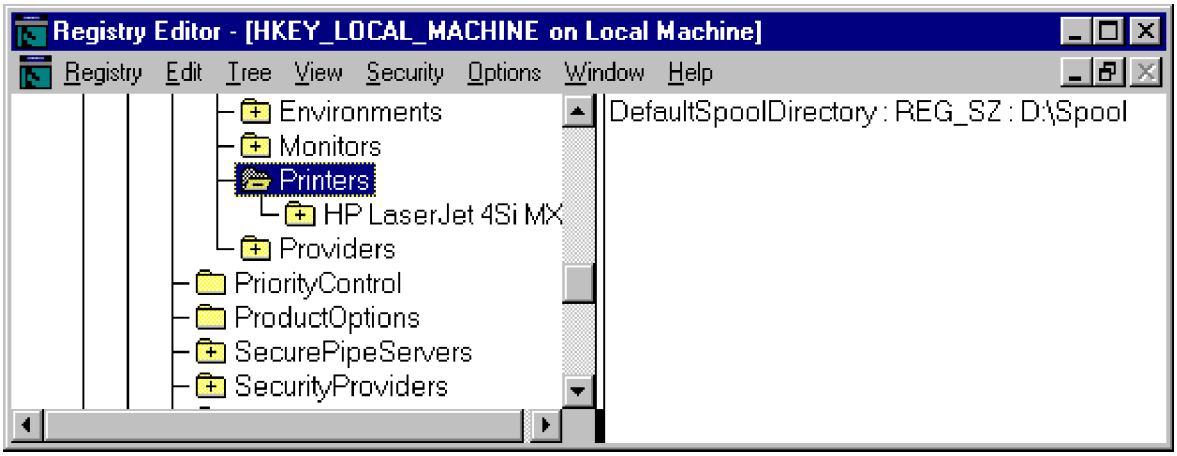
Rekisterin asetukset

Näitä kirjoittimien asetuksia voidaan määritellä myös suoraan rekisteriin.

Tulostusjonot

Tulostusjonojen käsittely voidaan ohjata muualle kuin oletuksena käytettävälle järjestelmälevylle:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Print\Printers**
Nimi	**DefaultSpoolDirectory**
Tyyppi	**REG_SZ**
Arvo	**[levyasema]:\[hakemisto]**



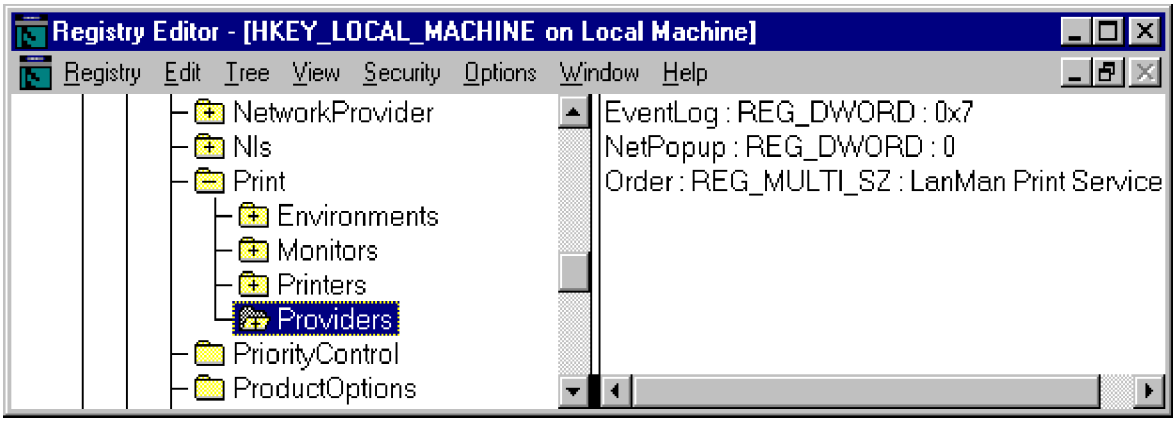
Asetus voidaan tehdä **Print Server**in **Advanced**-välilehdessä, mutta se sijaitsee samassa rekisterin kohdassa myös Windows NT 3.51:ssä.

Tulostusilmoitukset

Tulostusilmoitukset määritellään rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Print\Providers**
Nimi	**NetPopup**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei ilmoituksia, 1 - ilmoitukset tulevat (oletus)**

Asetus voidaan tehdä myös **Print Server**in **Advanced**-välilehdessä.



Tapahtumaloki

Tapahtumalokin merkinnät määritellään rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Print\Providers**
Nimi	**EventLog**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei merkintöjä, 7 - kaikki tapahtumat (oletus)**

Asetus voidaan tehdä myös **Print Server**in **Advanced**-välilehdessä.

Äänimerkki

Äänimerkki kuullaan oletuksena 10 sekunnin välein, kun työtä yritetään tulostaa uudelleen. Se määritellään rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Print\Providers**
Nimi	**BeepEnabled**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei merkkiääntä (oletus), 1 - merkkiääni**

Asetus voidaan tehdä myös **System Policy Editorilla** ja **Print Server**in **Advanced**-välilehdessä.

Selauksen esto

Voit estää NT-koneen kirjoittimien selailun:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Print**
Nimi	**DisableServerThread**
Tyyppi	**REG_DWORD**
Arvo	**0 - selailu sallittu (oletus), 1 - ei voi selata**

Asetus voidaan tehdä myös **System Policy Editorilla**.

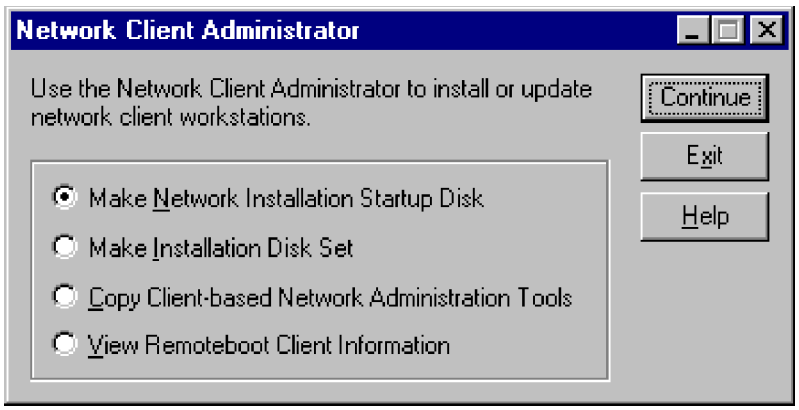
Network Client Administrator

Windows NT 4.0 Server-CD-ROM:illa on mm. Windows 95-asennushakemisto (US-versio). **Network Client Administrator**-ohjelman avulla voit tehdä verkkokäynnistyslevykkeen, jolla asennus sujuu verkon yli. Samaa verkkokäynnistyslevykettä voit käyttää muihinkin tarkoituksiin!

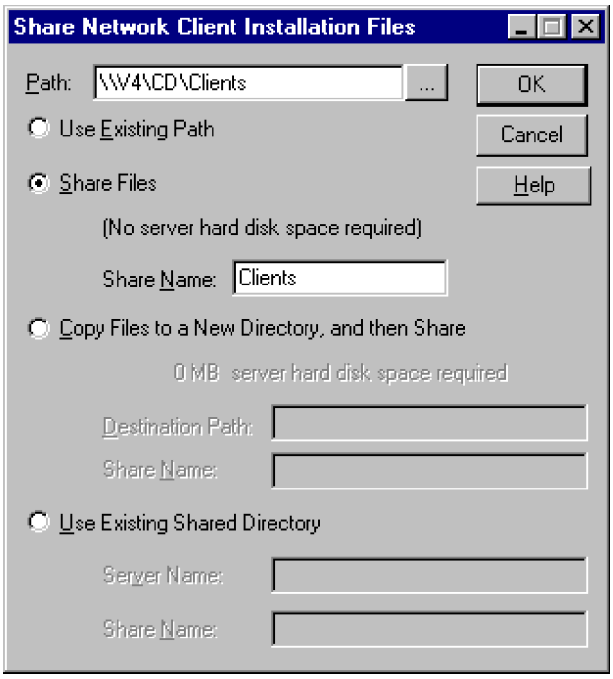
Alusta levyke MS-DOS- tai Windows 95-mikrossa komennolla **FORMAT A:/S**.

Tee näin:

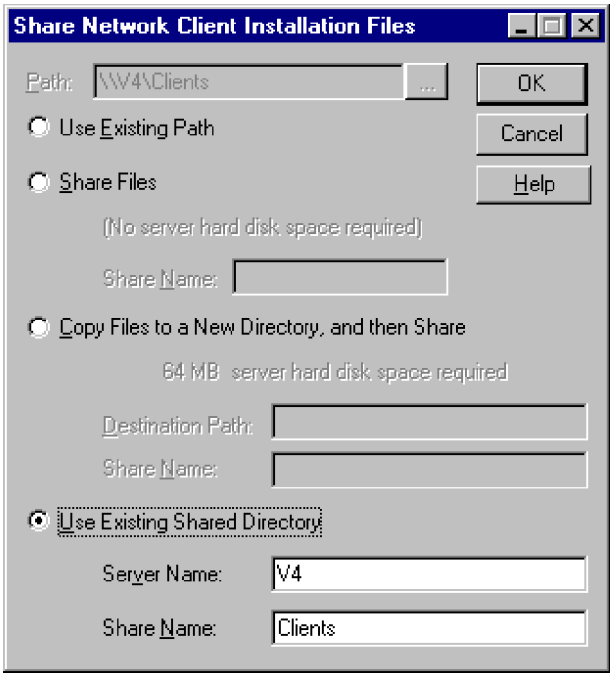
1) Käynnistä **Network Client Administrator**-ohjelma ja valitse **Make Network Installation Startup Disk**. Paina **Continue**



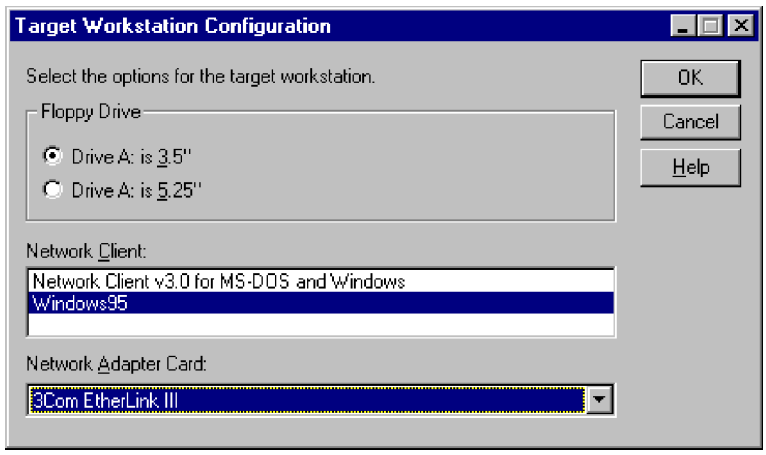
2) Määrittele, mistä Windows NT 4.0 Serverin CD-ROM:in Clients-hakemisto löytyy. Voit selata verkosta löytyvän hakemiston, tai verkkoon jaetun CD-ROM:in.



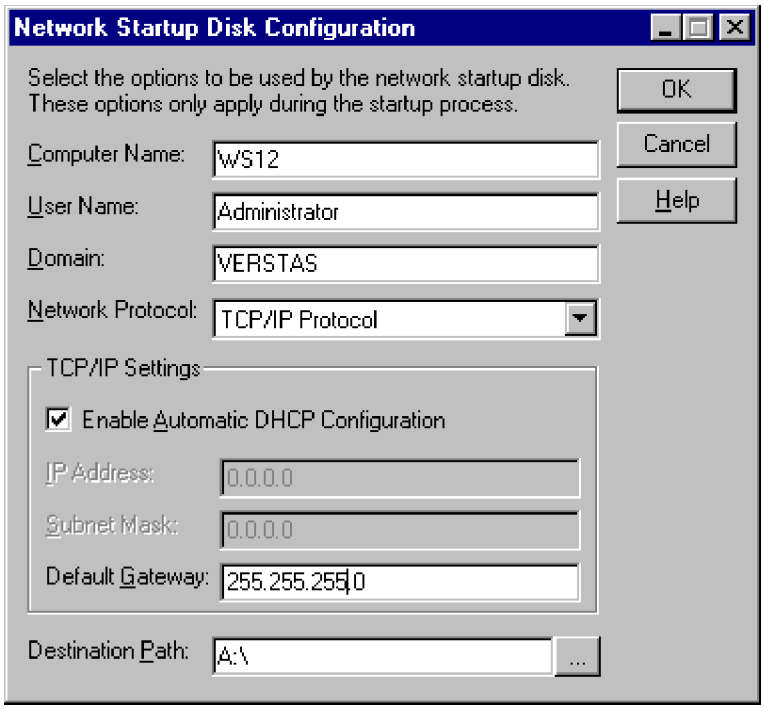
3) Riippuen Client-hakemiston jo luodusta jaosta, se jaetaan tai voit myös kopioida tiedostot palvelimen levylle valinnalla **Copy Files**. Jos jako on jo olemassa, voit valita **Share Files**. Tässä tapauksessa jako on **V4**-palvelimen **Clients**.



4) Määrittele, minkä työaseman haluat asentaa - MS-DOS:issa käytettävän **Network Client v3.0 for MS-DOS and Windows** (joka korvaa LAN Manager--työaseman) vai **Windows 95** (US-versio)



5) Määrittele lopuksi **asennuslevykkeen** tiedot. Jos valitset TCP/IP, voit valita myös DHCP:n, mikä helpottaa reititinverkossa tehtäviä asennuksia. Aseta levyke asemaan ja paina **OK**.



Dial-up Networking

Dial-up Networking-puhelinverkkoyhteyden avulla voit asentaa Windows NT-palvelimeen **Remote Access Service** (RAS)-etäkäyttöpalvelun. Se tukee 256 samanaikaista etäkäyttäjää, joiden pääsy verkkoon voidaan rajoittaa koskemaan vain etäkäyttöpalvelinta itseään.

RAS tukee seuraavia tietoliikenneyhteyksiä:

- Modeemi ja puhelinliitäntä
- ISDN-liitäntä
- X.25
- RS-232C-sarjaliikennekaapeli (nollamodeemikaapeli)

Remote Access Service (RAS)-etäkäyttöpalveluun liittyvät seuraavat komponentit:

- Ohjauspaneelin **Modems**, jolla määritellään käytettävien modeemien tyypit
- Ohjauspaneelin **Dial-up Monitor**, jolla valvotaan puheliverkkoyhteyksiä
- **Remote Access Admin**, jolla valvotaan etäkäyttöpalvelun käyttöä
- Ohjauspaneelin Network, jolla Remote Access Service voidaan asentaa ja konfiguroida
- **User Manager for Domains**, jolla annetaan käyttäjille etäkäyttöoikeudet
- **Dial-Up Networking**, jolla otetaan käyttöön etäkäyttöyhteys ja voidaan myös asentaa Remote Access Service.

Muistettavaa:

- Jos etäkäyttöpalvelin on liitetty lähiverkkoon, etäkäyttäjät voivat käyttää verkon palveluita aivan mikro olisi liitetty suoraan lähiverkkoon. Muista, että oikeus kirjautua toimialueelle etäyhteyden kautta on erikseen annettava käyttäjäkohtaisesti!

- Tukihenkilöt voivat hallita verkon palvelimia vaikkapa kannettavasta mikrosta, jossa on GSM-datakorttiin kytketty GSM-matkapuhelin. Windows NT-palvelimien hallintaan tarvittavat Windows NT -työasemaversiot löytyvät Windows NT 4.0 -palvelimen CD-ROM:in **Clients\Srvtools\Winnt**-hakemistosta ja Windows 95 -ohjelmat **Clients\Srvtools\Win95**-hakemistosta

- RAS-palvelu vaatii ennen kaikkea **muistia** palvelimesta. 128 Mt keskusmuistilla varustettu RAS-palvelin ei ole mitenkään harvinainen. Toisaalta palvelimen prosessori voi olla mainiosti vain Pentium/100 MHz

- Jos käytyt RAS-palveluun palvelimen omia **sarjaportteja**, RAS-palvelu kuormittaa prosessoria huomattavasti! Raskaassa käytössä on ehdottoman suositeltavaa asentaa jokin sarjaporttilaajennin palvelimeen!

- RAS-palvelu käynnistyy automaattisesti, asetus hallitaan Ohjauspaneelin **Services**- kuvakkeella. RAS-palvelun voi myös käynnistää ja lopettaa **Remote Access Admin**-ohjelmassa komennolla **Server | Start Remote Access Service**

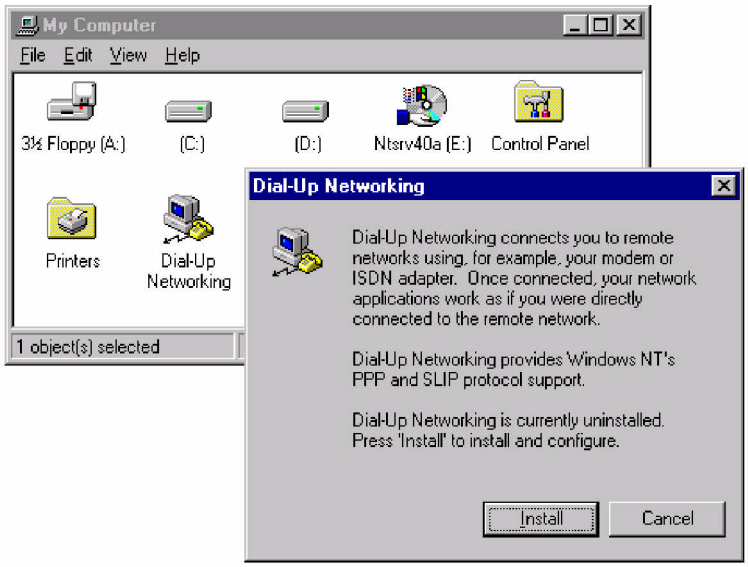
- Jos jokin modeemi ei ole käytettävissä RAS-palvelun käynnistyessä, se yrittää muutaman sekunnin välein kytkeytyä porttiin. Tästä seuraa myös levykuormitusta!

- Jos päivität Windows NT 3.5x:n Windows NT 4.0:aan, niin modeemien asetukset luetaan aiemmasta asennuksesta. Jos kyseessä on uusi asennus, niin modeemeille asennetaan oletuksena **unimodem**-tuki. Jos modeemisi ei tue unimodemia, joudut poistamaan tuen rekisteristä.

Käyttöönotto

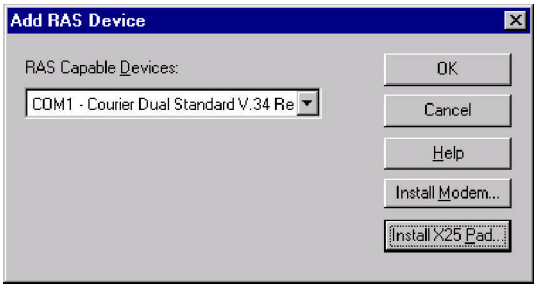
Helpoin menetelmä on valita **Dial-Up Networking**-kuvake **My Computer**-ikkunassa. Toinen menetelmä on Ohjauspaneelin **Network**-kuvakkeen **Services**-välilehti. Valitse **Remote Access Service**-palvelu.

1) Aloita asennus painamalla **Install**.

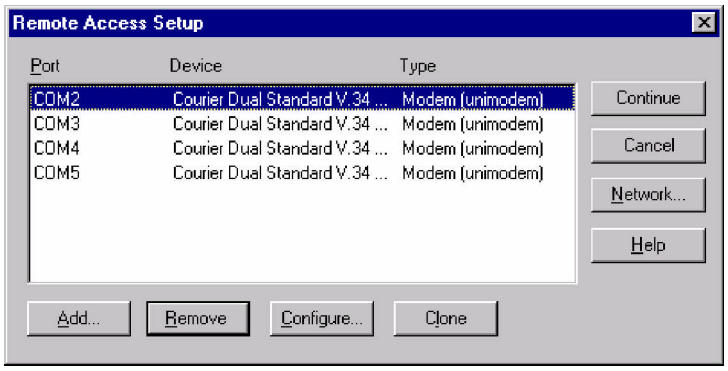


2) Jos RAS:in tukemaa oheislaitetta (esimerkiksi modeemia) ei ole asennettu, se asennetaan seuraavaksi. Modeemin asentamisen voit katsoa Ohjauspaneelista, luku **3**.

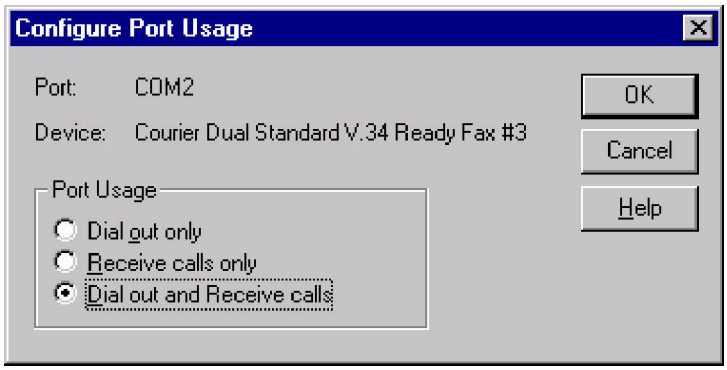
3) Anna tämän jälkeen sarjaportti ja modeemi, jota haluat käyttää - jos modeemia ei ole asennettu, valitse **Install modem**:



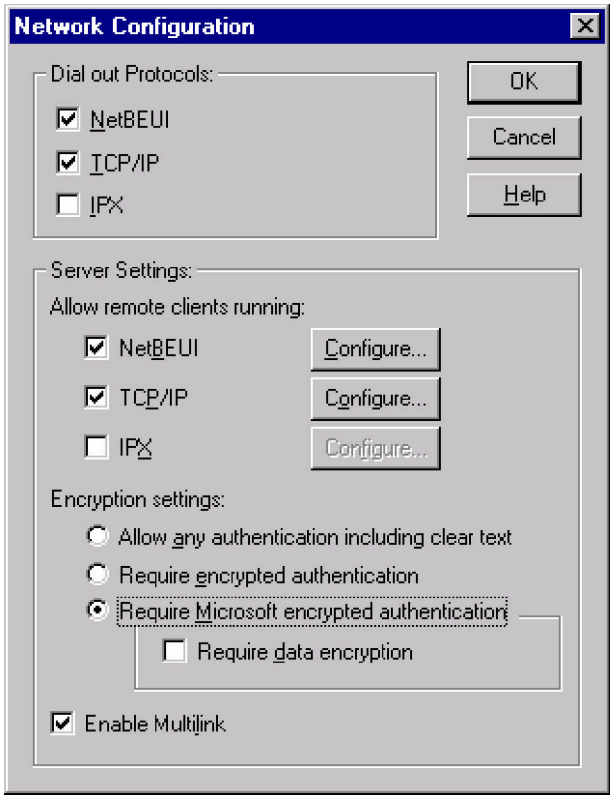
4) Paina **OK** ja anna käytettäville modeemeille oikeat asetukset painamalla **Configure**.



5) **Configure Port Usage**-asetuksissa määritellään, miten modeemi toimii; voidaanko soittaa vain ulos (**Dial out only**), ottaa vastaan vain tulevat soitot (**Receive calls only**) vai molempia (**Dial out and Receive calls**).



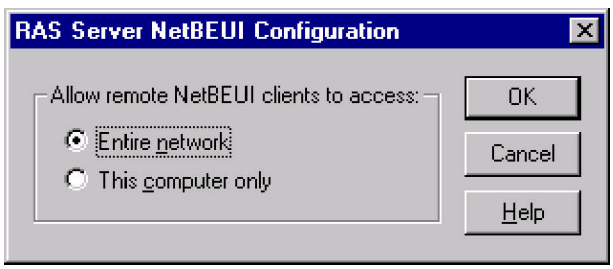
6) Valitsemalla **Network** voidaan määrittää käytettävät protokollat ja salasanojen salakirjoitustapa:



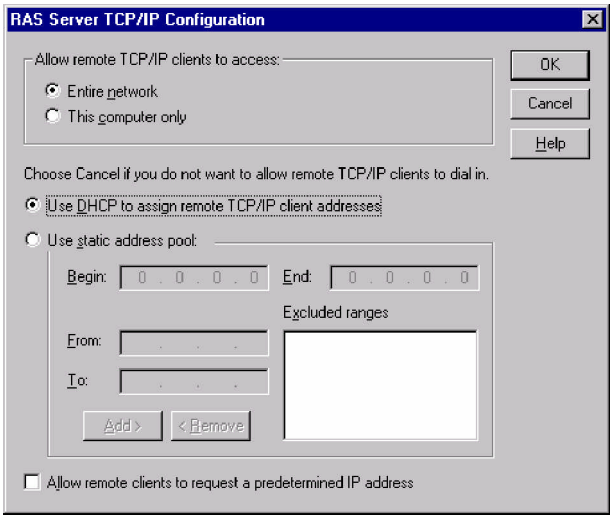
Valinnat ovat seuraavat:

- Jos etäkäytetään **Novell NetWare**-palvelimia, tarvitaan **IPX**-protokollaa. IPX:n asetuksilla määritellään mm. IPX:n sisäisen verkkonumeron käyttö sekä pääseekö käyttäjä koko verkkoon (**Entire network**) vai **ainoastaan etäkäyttöpalvelua tarjoavaan tietokoneeseen** (**This computer only**)

- NetBEUI:n asetuksilla voit myös määritellä pääseekö etäkäyttäjä protokollalla koko verkkoon vai ainoastaan etäkäyttöpalvelua tarjoavaan palvelimeen



- TCP/IP:n asetuksissa samoin voidaan määritellä pääsy verkkoon ja osoitteiden jakelu voidaan hoitaa DHCP-palvelun avulla. Tällöin ei tarvitse määritellä kyseisen verkon TCP/IP-asetuksia etätyöasemissa, riittää, kun niissä on määritelty käyttöön DHCP:n käyttö. Jos et halua käyttää DHCP:tä, voit myös valita käyttöön **etäkäyttö-palvelimen** jakaman kiinteän IP-osoiteavaruuden.



7) Paina lopuksi **Continue**. Tarvittavat protokollat ja sidokset luodaan sekä etäkäyttöpalvelu asennetaan. Lopuksi palvelin käynnistetään uudelleen.

Rekisterin asetukset

Rekisterissä on joitakin palvelua ohjaavia asetuksia, joita kannattaa tarvittaessa muuttaa:

- **AuthenticateRetries** asettaa montako epäonnistunutta kirjautumisyritystä sallitaan. Arvoa voi muuttaa myös **Policy Editorilla**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\RemoteAccess\Parameters**
Nimi	**AuthenticateRetries**
Tyyppi	**REG_DWORD**
Arvo	**0 - 10, oletus 2**

- **AuthenticateTime** määrittelee, minkä ajan kuluessa käyttäjän on kirjauduttava RAS-palvelun kautta. Arvoa voi muuttaa myös **Policy Editorilla**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\RemoteAccess\Parameters**
Nimi	**AuthenticateTime**
Tyyppi	**REG_DWORD**
Arvo	**20 - 600 sekuntia, oletus 120 sekuntia**

- **CallbackTime** on aika, jonka RAS-palvelin odottaa ennen takaisinsoittoa, **jos** työasema ei ilmoita muuta odotusaikaa:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\RemoteAccess\Parameters**
Nimi	**CallbackTime**
Tyyppi	**REG_DWORD**
Arvo	**2 -12 sekuntia, oletus 2 sekuntia**

- **EnableAudit** määrittelee, kirjataanko RAS-palvelun tapahtumat lokiin:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\RemoteAccess\Parameters**
Nimi	**EnableAudit**
Tyyppi	**REG_DWORD**
Arvo	**0 (ei kirjata), 1 kirjataan (oletus)**

Käyttäjän kannalta tarpeellinen RAS-asetus on **KeepRasConnections**, jolla määritellään katkaistaanko yhteys käyttäjän poiskirjautumisen yhteydessä. Asetus annetaan **NT-työasemassa**:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\WindowsNT\CurrentVersion\Winlogon**
Nimi	**KeepRasConnections**
Tyyppi	**REG_SZ**
Arvo	**0 - yhteys katkaistaan (oletus), 1 - yhteyttä ei katkaista**

Valvonta

RAS-palvelun valvontaan on NT:n mukana kaksi työkalua, ja Resource Kitissä muutama lisää.

Dial-up Monitor

Ohjauspaneelin **Dial-up Monitor**in avulla valvotaan puhelinverkko-yhteyksien tilaa. Käytettävissä on kolme välilehteä:

- **Status** kertoo tämän hetkisen tilan lähetetyistä ja vastaan-otetuista tavuista, virheiden määrän ja linjan tilan

- **Summary** on multilink-linjojen yhteenveto eli samanaikaisesti yhteen kohteeseen käytettyjen linjojen tila

- **Preferences** määrittelee äänimerkit virhetilanteissa ja tehtäväpalkin indikaattorin asetukset.

Remote Access Admin

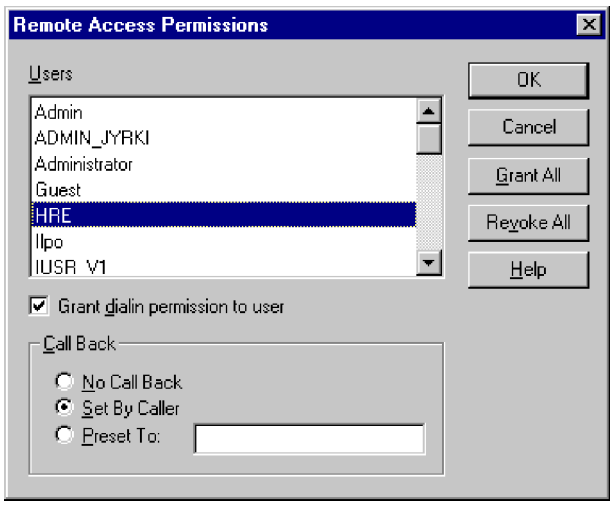
Remote Access Admin-ohjelmalla valvotaan itse etäkäyttöpalvelun käyttöä. Käyttäjän yhteyden aikana voit käyttää seuraavia toimintoja:

- **Users**-valikon **Active Users** kertoo kuka tällä hetkellä käyttää etäkäyttöpalvelua. Kun valitset edellisen valikon kohdan **User Account**, saat esille tarkemmat käyttäjätiedot: käyttäjätunnuksen, koko nimen, salasanan asetukset, käyttöoikeustason ja takaisinsoittoasetukset

- **Server**-valikon kohdasta **Communication Ports** saat esille sarjaliikenneporttien sen hetkisen tilan ja myös mahdolliset käyttäjät. Samoin voit halutessasi lähettää heille viestin (**Send Message**) tai tipauttaa pois linjoilta (**Disconnect User**)

- **Port Status** kertoo tietoja kyseisen portin käyttäjästä.

Users-valikon **Remote Access Permissions** avulla voidaan halutuille käyttäjille antaa oikeus etäkäyttöön - se tehdään laittamalla rasti ruutuun **Grant dialin permission to user**.



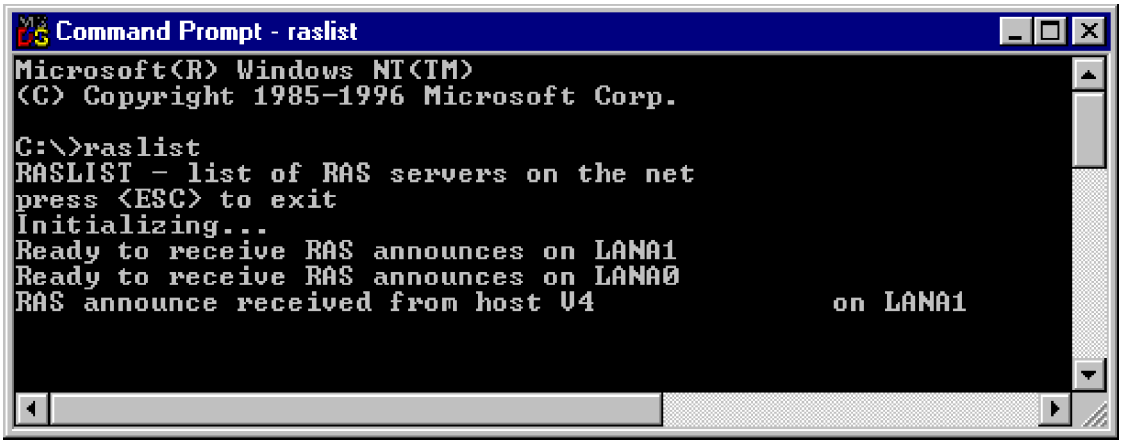
Kohta **Callback** määrittää, mitä takaisinsoiton kanssa tehdään:

- **No Call Back** - ei mahdollista takaisinsoittoa lainkaan
- **Set By Caller** - mahdollistaa yhteysvaiheessa takaisinsoiton käyttäjän siinä vaiheessa antamaan numeroon
- **Preset to** soittaa aina annettuun numeroon ja on tietoturvan kannalta luotettavin vaihtoehto.

User Manager for Domainsilla voit antaa etäkäyttöoikeudet useammalle käyttäjälle samanaikaisesti.

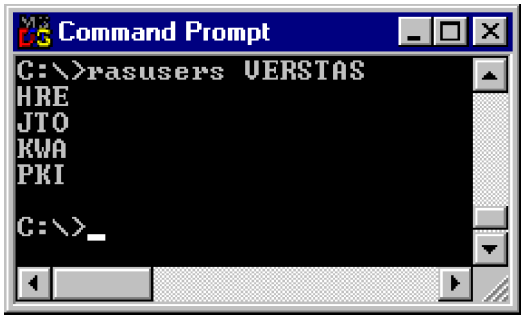
RASLIST

RASLIST.EXE on Resource Kitin apuohjelma, joka etsii verkon kautta RAS-palvelimia. Näin voidaan tutkia, onko kenties Windows NT-työasemissa RAS-palvelu käynnissä.



RASUSERS

RASUSERS on Resource Kitin apuohjelma, joka etsii käyttäjät, joilla on oikeus kirjautua etäyhteyden kautta. Valitsimena annetaan toimialueen tai palvelimen nimi.



Remote Access Manager

Remote Access Manager on **liquid vision**in ohjelma, jonka kahden portin versio tulee Resource Kitin mukana. Sen voi asentaa Resource Kitin päävalikosta tai **APPS\RASMGR**-hakemistosta.

Apuohjelmia palvelimien hallintaan

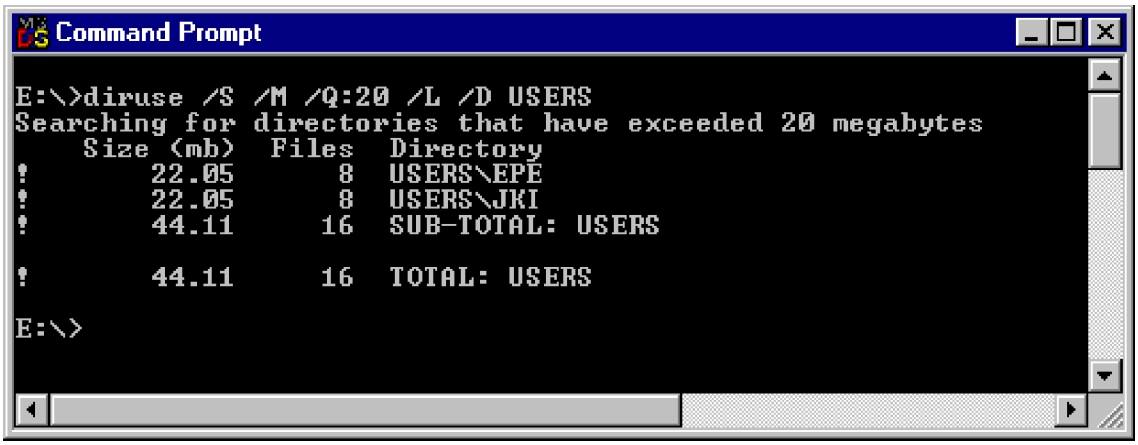
Seuraavaksi käsitellään **Windows NT 4.0 Server Resource Kit**in mukana tulevia työkaluja palvelinten hallintaan.

Vastaavia apuohjelmia löytyy kosolti internetistä. Käyttöönotossa kannattaa olla varovainen - kukaan ei todennäköisesti vastaa ongelmatilanteissa mihinkään kysymyksiin.

Tyypillisesti nämä ohjelmat edellyttävät **Administrator**-tason oikeuksia tai **Server Operators**-ryhmän jäsenyyttä kohteessa.

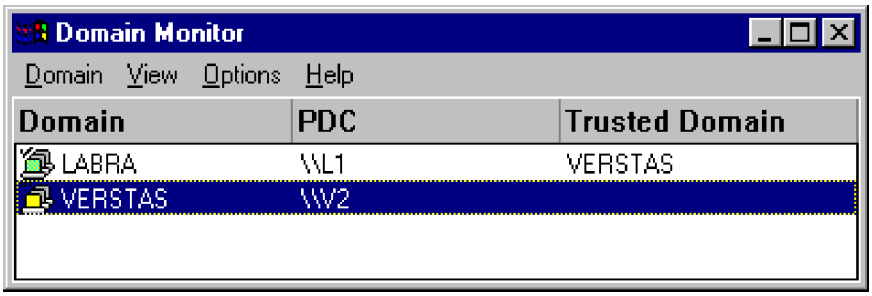
DIRUSE

Microsoftilta ei edelleenkään ole tullut Windows NT:lle levytilan valvontaa (Quota), mutta **DIRUSE**-apuohjelmalla saa listan hakemistoista, jotka ovat ylittäneet annetun koon. Esimerkissä **DIRUSE**-komennon valitsimet määrittelevät listauksen kohteeksi ne **USERS**-hakemiston alihakemistot, joiden koko **ylittää 20 megatavua**. Samalla kirjoitetaan loki. Hälytys saadaan haluttaessa /**A**-valitsimella.

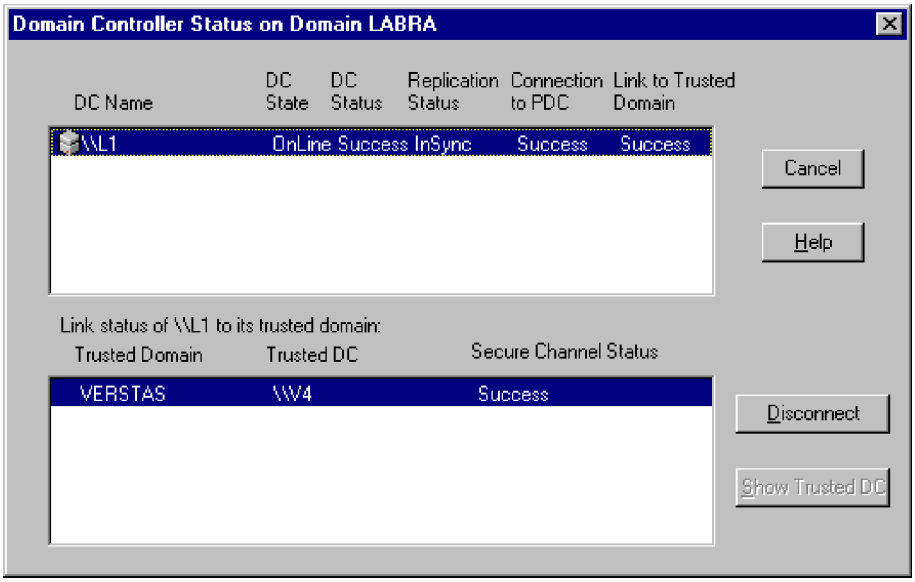


Domain Monitor

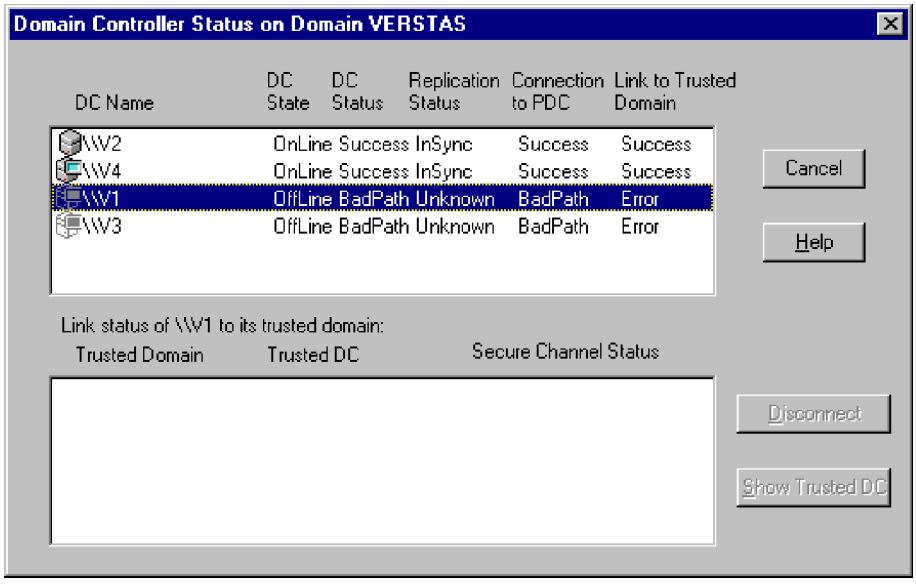
DOMMON-apuohjelman avulla voidaan valvoa luottosuhteita sekä palvelimien välistä käyttäjätietokannan synkronointia.



Tässä esimerkissä **LABRA**-toimialueelta on luottosuhde **VERSTAS**-toimialueelle. Valitsemalla kohteeksi **LABRA**-toimialue nähdään että VERSTAS-toimialueella luottosuhdetta ylläpitää palvelin **V4**.



Valitsemalla kohteeksi **VERSTAS**-toimialue nähdään VERSTAS-toimialueen ohjauskoneiden synkronointitilanne. Palvelimet **V1** ja **V3** eivät ole synkronoitu pääohjauskoneen kanssa.



FREEDISK

FREEDISK tutkii, onko kohteessa vapaata levytilaa annetun parametrin verran (tavuina). Jos on se, antaa paluuarvon **0**.

Esimerkki tietokannan kopioivasta komentojonosta:

```
FREEDISK E: 2048000000
IF ERRORLEVEL 0 GOTO COPYDB
EXIT
:COPYDB
COPY D:\MSSQL\DATA\MASTER.DB E:\
```

INSTSRV

INSTSRV-apuohjelman avulla voit asentaa palveluita.

Syntaksi on:

```
INSTSRV <palvelun nimi> (<EXE-tiedosto> | REMOVE)
[-a <käyttäjätunnus>] [-p <Salasana>]
```

Esimerkiksi **BX.EXE** voidaan asentaa palveluksi komennolla:

```
INSTSRV BX E:\APPS\BX.EXE -a VERSTAS\ADMIN -p PUKKI
```

Tarkista myös Ohjauspaneelin **Service**-valintaikkunasta palvelun käynnistysasetukset. Myös komentorivin **NET START**-komentoa voi käyttää.

Palvelu voidaan poistaa komennolla:

```
INSTSRV  BX  REMOVE
```

NETSVC

NETSVC-apuohjelmalla voit käynnistää tai pysäyttää palveluita toisissa NT-koneissa.

Syntaksi on:

NETSVC palvelunimi \\konenimi /komento

jossa komento voi olla:

/query	kysely palvelun tilasta
/start	palvelun käynnistys
/stop	palvelun pysäytys
/pause	palvelun keskeytys
/continue	keskeytetyn palvelun jatkaminen
/list	luettelo asennetuista palveluista

Komentojono, joka tutkii, jos WWW-palvelin on pysäytetty palvelimessa **V4**; jos on, se käynnistetään:

```
@ECHO OFF
NETSVC  W3SVC  \\V4  /QUERY > C:\TEMP\T.TXT
FINDSTR  /C:stopped  C:\TEMP\T.TXT
IF ERRORLEVEL 0  NETSVC  W3SVC  \\V4  /START
```

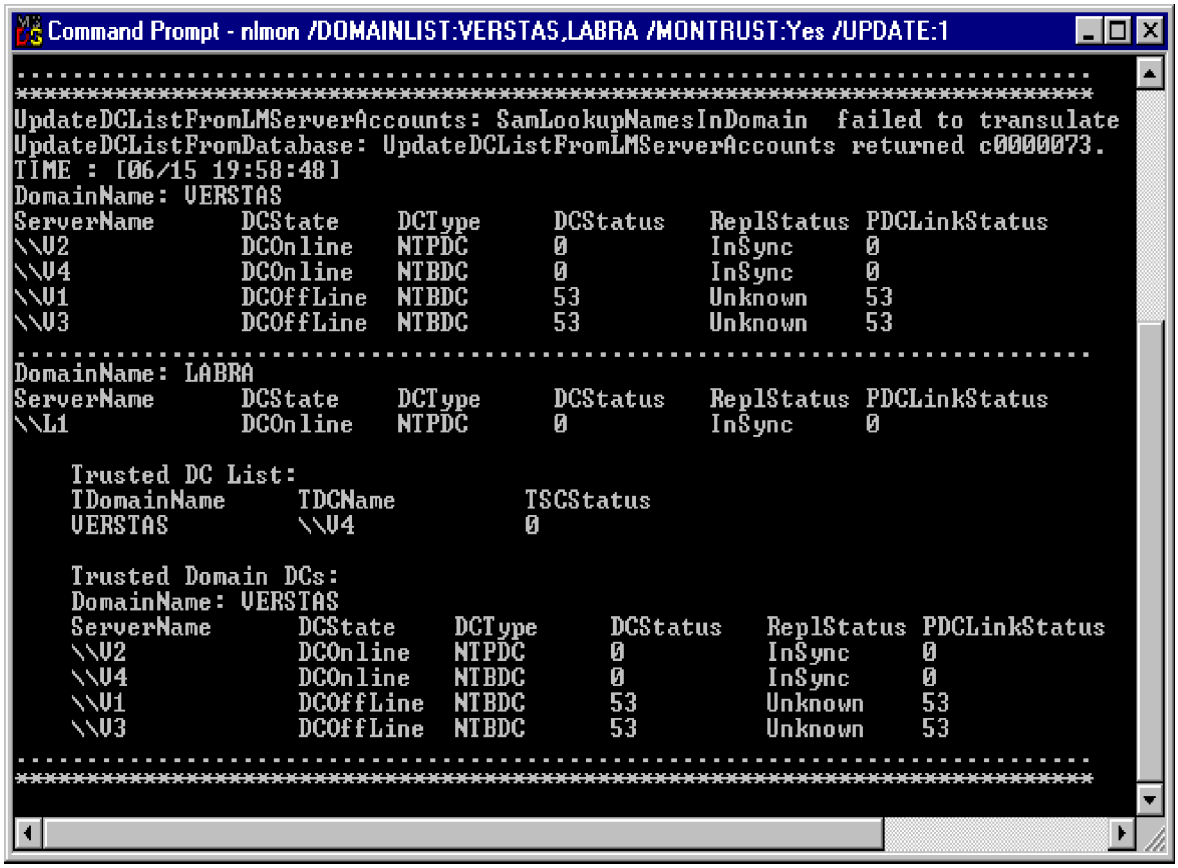
Tätä voi käyttää hyväksi toimittaessa ongelmallisen palvelimen kanssa.

NLMON

NLMON-apuohjelmalla voidaan valvoa luottosuhteita sekä toimialueen ohjauskoneiden synkronointia. Ohjelma tukeutuu selauspalveluun, joten selauksen on oltava kunnossa.

Esimerkissä tarkkaillaan toimialuiden **LABRA** ja **VERSTAS** välistä luottosuhdetta sekä toimialueen **VERSTAS** ohjauskoneiden synkronointia:

- **DCType** NTPDC on pääohjauskone (PDC)
- **DCType** NTBDC on varaohjauskone (BDC)
- **DCStatus** 53 kertoo, etteivät asiat ole tolallaan
- **Trusted DC List** kertoo, että LABRA-toimialueen luottosuhde VERSTAS-toimialueelle on muodostettu palvelimen **V4** kautta



NLTEST

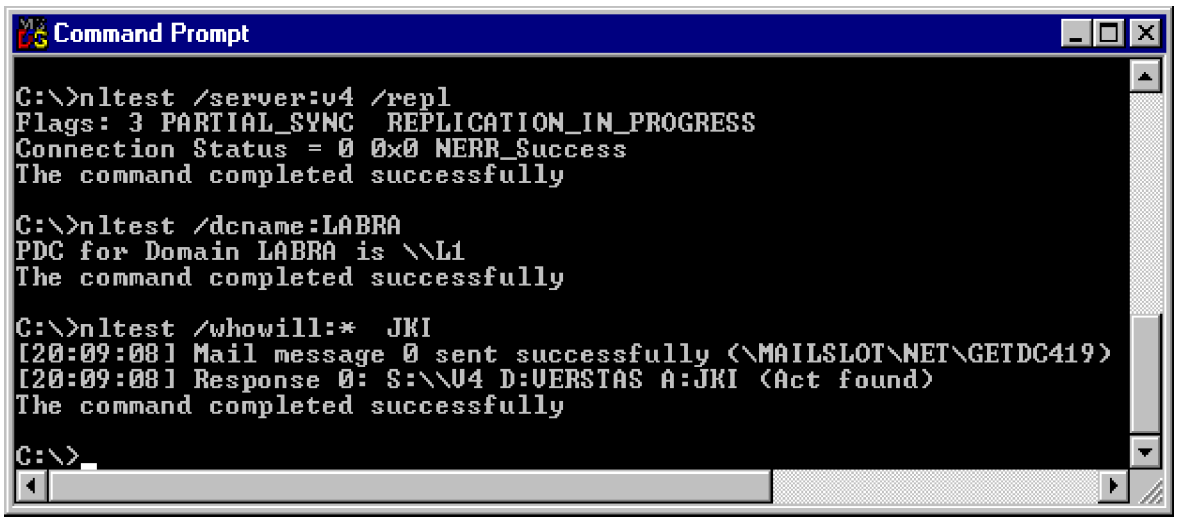
NLTEST on monipuolinen apuohjelma, jolla voidaan synkronoida toimialue, kysellä käyttäjätietoja, kysyä palvelimien rooleja, tarkistaa toimialuieden kokoonpanoja jne.

Joitakin esimerkkejä:

Käyttäjätietokannan kopiointi palvelimelle **V4**:
NLTEST /SERVER:V4 /REPL

Toimialueen LABRA PDC:
NLTEST /DCNAME:LABRA

Löytyykö käyttäjätunnus JKI:
NLTEST /WHOWILL:* JKI



PERMS

PERMS-apuohjelma tarkistaa käyttäjän oikeudet kohteessa. Syntaksi on:

PERMS käyttäjätunnus kohde /I /S

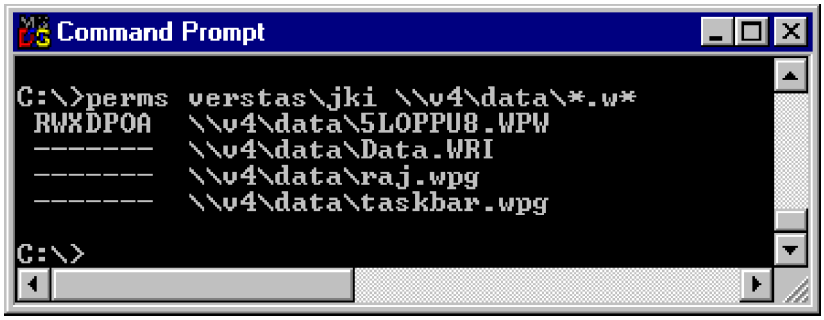
Valitsimet:

/S - tarkistetaan myös alihakemistot

/I - tarkistetaan myös vuorovaikutteisen käyttäjän (Interactive) oikeudet.

Esimerkiksi **VERSTAS**-toimialueen käyttäjäntunnuksen **JKI** oikeudet **V4**-palvelimen **DATA**-hakemiston kaikkiin tyypiltään **W**-alkuisiin tiedostoihin:

PERMS VERSTAS\JKI \\V4\DATA*.W*



Vastaus nähdään oikeuksia vastaavina kirjaimina:

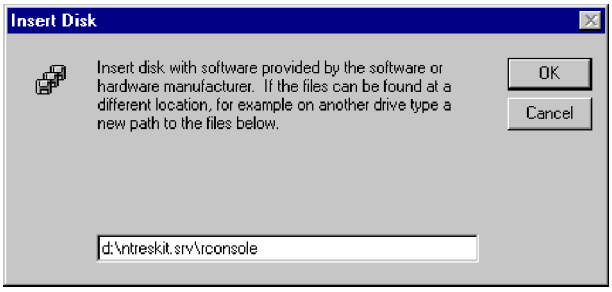
R Read
W Write
X Execute
D Delete
P Change Permissions
O Take Ownership
A General All
- No Access

Remote Console

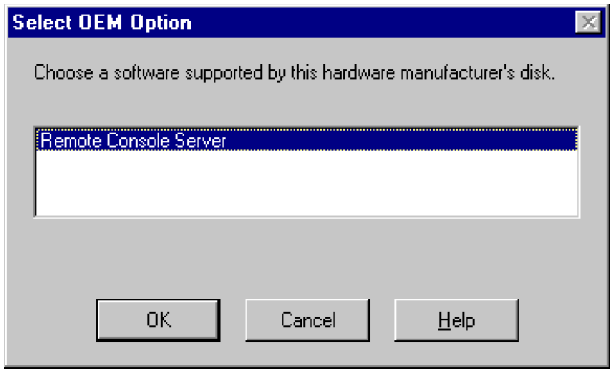
Remote Console on palvelu, joka mahdollistaa palvelimen komentorivin siirron toiseen NT-koneeseen. Palvelu käynnistää paikallisen **CMD.EXE**-prosessin jokaiseen yhteyteen, joka näyttö siirretään toiseen NT-koneeseen. Paikallisen käyttäjän ei tarvitse olla kirjautuneena palvelimelle.

Asennus palvelimeen tehdään seuraavasti:

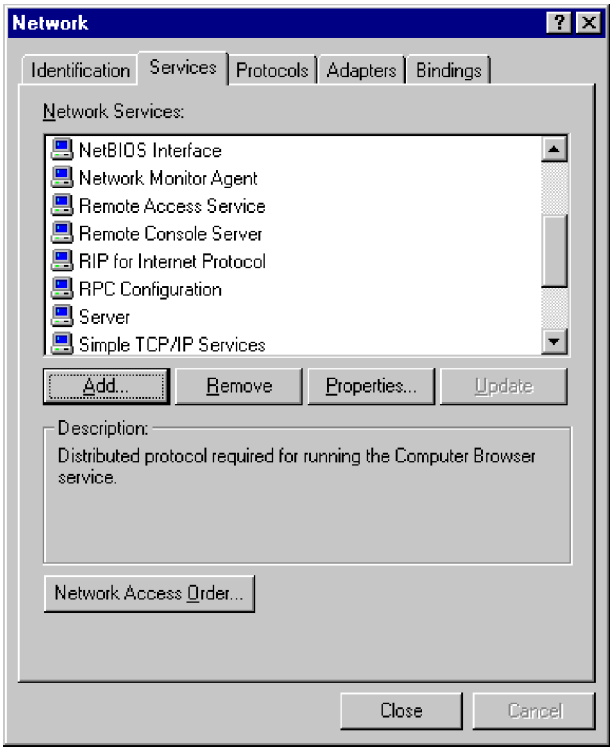
1) Avaa Ohjauspaneelissa **Network** ja valitse **Services**-välilehti. Paina **Have Disk** ja selaa Resource Kitin **RConsole**-hakemisto:



2) Valitse **Remote Console Server**

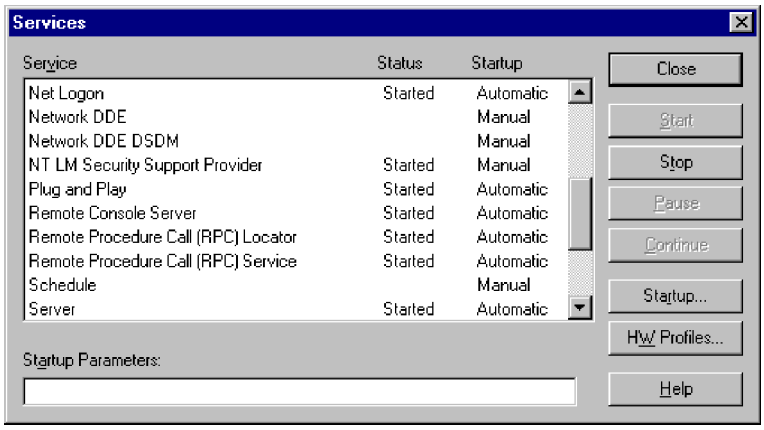


3) Valinta tulee asennettujen verkkopalveluiden listalle:



4) Paina **OK** ja käynnistä palvelin uudelleen.

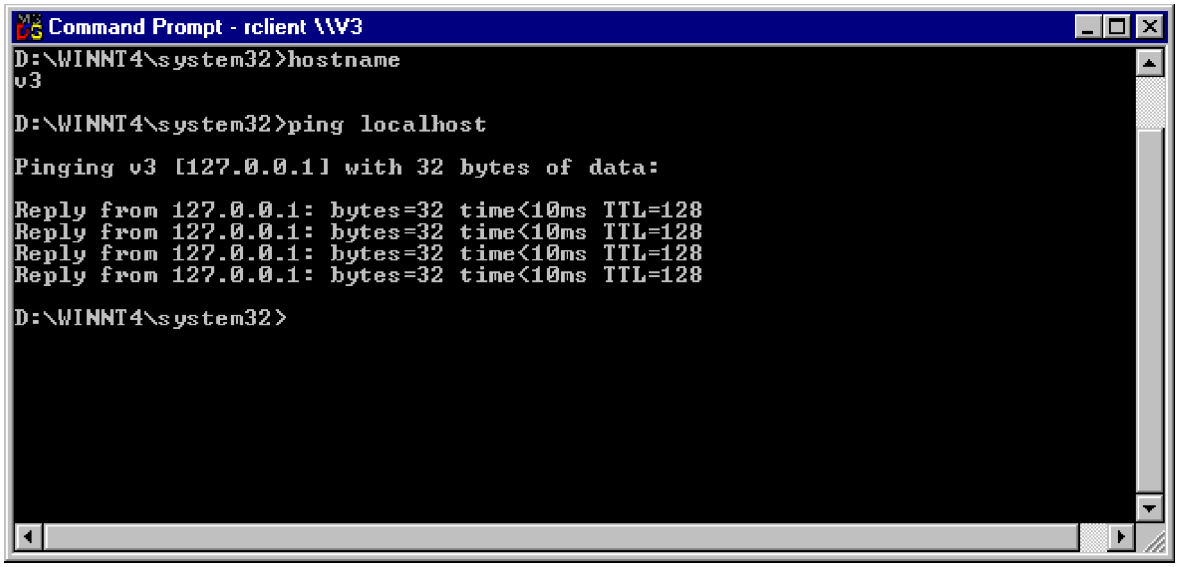
Remote Console Service on palveluiden luettelossa.



Toisessa NT-koneessa yhteys muodostetaan komennolla:

RCLIENT [\\]palvelin

Esimerkiksi **HOSTNAME** ja **PING**:



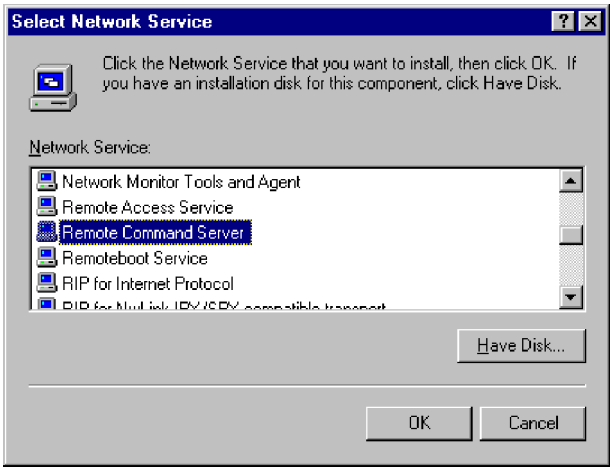
Remote Command Service

Remote Command Service (**RCMDSVC.EXE**) on vastaavantyyppinen kuin **Remote Console**, mutta tässä komentorivi ohjataan paikallisesta NT-koneesta palvelimelle.

RCMDSVC.EXE on palvelimen palvelu, ja se asennetaan NT-palvelimeen esimerkiksi seuraavasti:

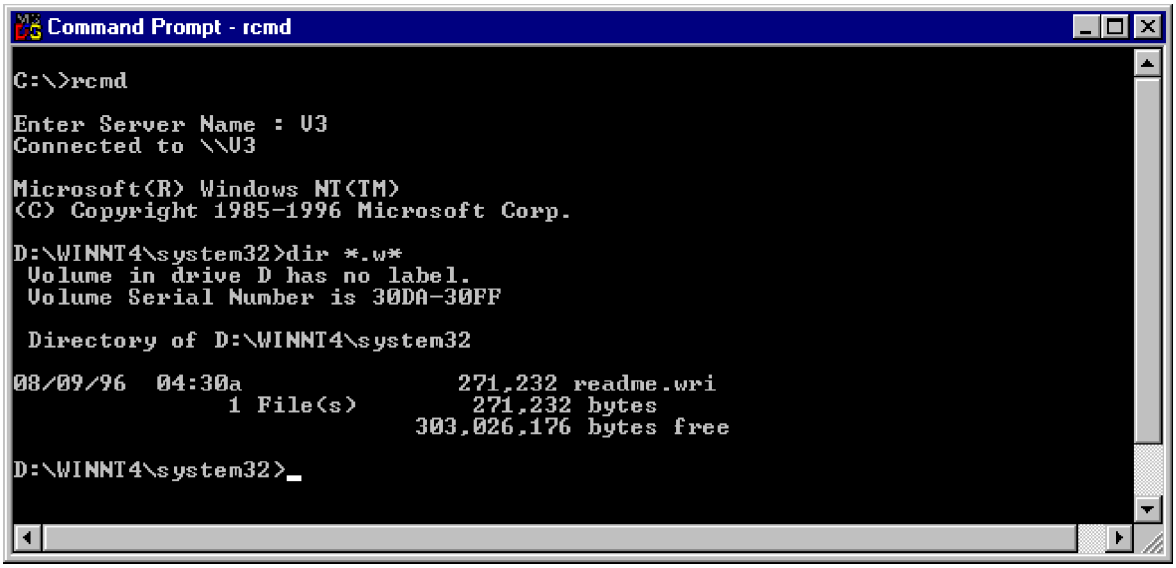
1) Kopioi **RCMDSVC.EXE**- ja **OEMNSVRC.INF**-tiedostot **%SYSTEMROOT%\SYSTEM32** -kansioon

2) Avaa Ohjauspaneelissa **Network** ja valitse **Services**-välilehti. Paina **Add** ja valitse **Remote Command Server**



3) Käynnistä palvelu Ohjauspaneelissa **Services**-kuvakkeen avulla. Valitse **Remote Command Server** ja paina **Start**.

Toisessa NT-koneessa voidaan käynnistää **RCMD.EXE**. Lisäksi on annettava palvelimen nimi, ja sitten päästäänkin käsiksi palvelimen komentoriville.



Remote Kill

Remote Kill (**RKILLSRV.EXE**) on palvelu, joka mahdollistaa prosessien etähallinnan. Käytettävissä on Windows-sovellus **WRKILL.EXE** ja komentorivi **RKILL.EXE**.

Palvelun voi asentaa joko **INSTSRV.EXE**:llä tai **SRVINSTW.EXE**:llä.

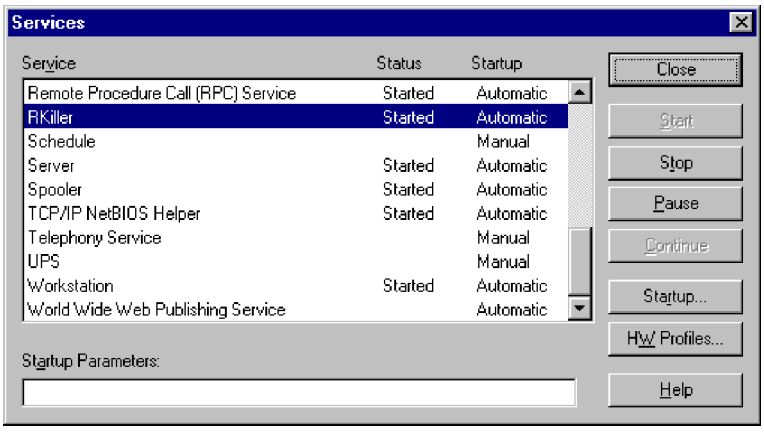
INSTSRV.EXE:ä käytettäessä komento on

INSTSRV palvelun_nimi RKILLSRV.EXE -a käyttäjätunnus -p Salasana

esimerkiksi:

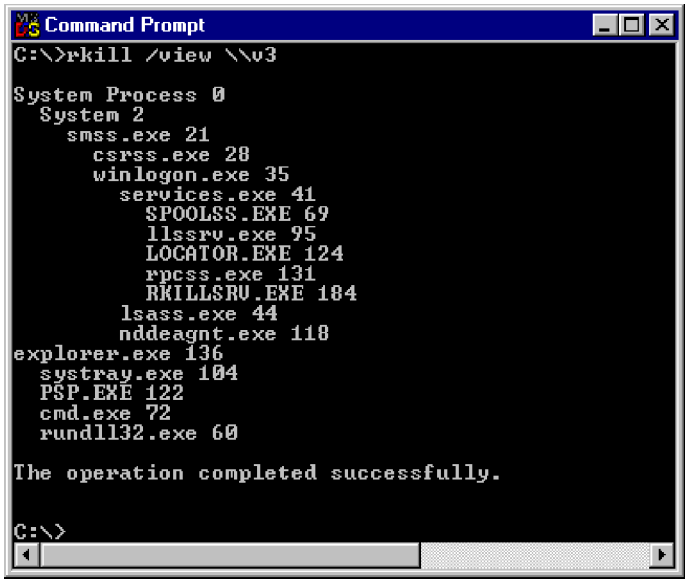
INSTSRV Rkiller D:\RESKIT4\RKILLSRV.EXE -a VERSTAS\Admin -p x2yz

Käyttäjätunnuksella on oltava oikeus **Log On As a Service**.



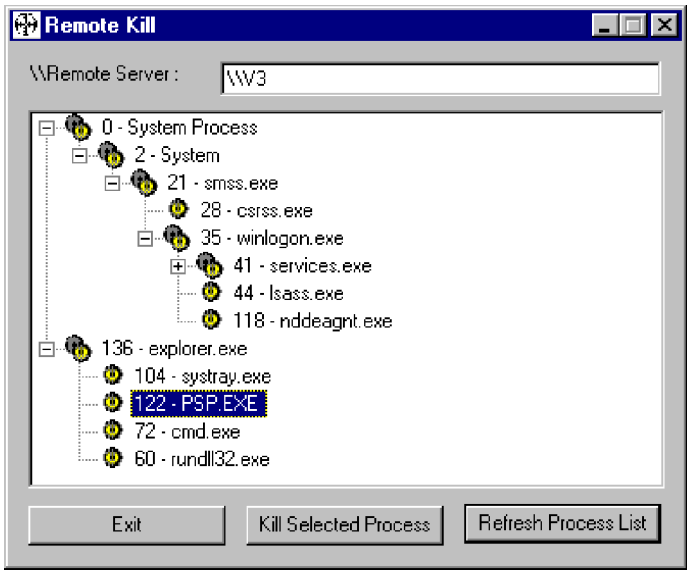
Käynnistä palvelu Ohjauspaneelissa **Services**-kuvakkeen avulla. Valitse **Rkiller** ja paina **Start**.

Tämän jälkeen voit käyttää komentorivin **RKILL**-komentoa hallitaksesi kohteen prosesseja.



Komennolla **RKILL /VIEW \\palvelin** näet kohteen prosessit, ja komennolla **RKILL /KILL \\palvelin prosessin_id** voit lopettaa prosessin. Edellisessä esimerkissä **PSP.EXE** lopetaan komennolla **RKILL /KILL \\V3 122**.

Komennolla **WRKILL** käynnistyy Windows-versio. Valitsemalla kohteen näet sen prosessit, ja **PSP.EXE** lopetaan valitsemalla se ja painamalla **Kill Selected Process**.



RMTSHARE

RMTSHARE on ohjelma, jolla voidaan jakaa komentoriviltä etäkoneen hakemistoja, samalla voidaan antaa jaetulle hakemistolle käyttöoikeudet verkon kautta.

Syntaksi on:

```
RMTSHARE  \\palvelin

        \\palvelin\jakonimi

        \\palvelin\jakonimi=levyasema:polku [/USERS:lkm | /UNLIMITED]
                [/REMARK:"teksti"]
                [/GRANT [käyttäjä[:oikeus][ /GRANT [käyttäjä[:oikeus]]]
                [/REMOVE käyttäjä]

        \\palvelin\jakonimi=kirjoitinnimi  /PRINTER [/USERS:lkm |
                 UNLIMITED]
                 [/REMARK:"teksti"]
                 [/GRANT [käyttäjä[:oikeus][ /GRANT [käyttäjä[:oikeus]]]
                 [/REMOVE käyttäjä]

        \\palvelin\jakonimi [/USERS:lkm | /UNLIMITED]
                 [/REMARK:"tekstit"]
                 [/GRANT [käyttäjä[:oikeus][ /GRANT [käyttäjä[:oikeus]]]
                 [/REMOVE käyttäjä]

        \\palvelin\jakonimi /DELETE
```

Esimerkkejä:

Jaetaan **V3**-palvelimen **DATA**-hakemisto siten, että **Everyone**-ryhmä saa lukuoikeudet:

```
RMTSHARE  \\V3\DATA=E:\DATA  /GRANT EVERYONE:R
```

Jakaminen lopetetaan komennolla:

```
RMTSHARE  \\V3\DATA /DELETE
```

Lokien hakemiston jakaminen väliaikaisesti tallennusta varten komentojonon avulla:

```
RMTSHARE  \\V5\LOKIT=E:\LOKIT  /GRANT EVERYONE:F
COPY  \\V1\LOKIT\*.LOG  \\V5\LOKIT\*.*
RMTSHARE   \\V3\DATA  /DELETE
```

Tarkistetaan onko **DATA**-hakemisto jaettu **V3**-palvelimelta; jos ei se, jaetaan **Everyone**-ryhmälle lukuoikeuksin:

```
@ECHO OFF
NET USE R: /D
NET USE R: \\V3\DATA
IF NOT EXIST R:\NUL RMTSHARE \\V3\DATA=D:\DATA /G EVERYONE:R
```

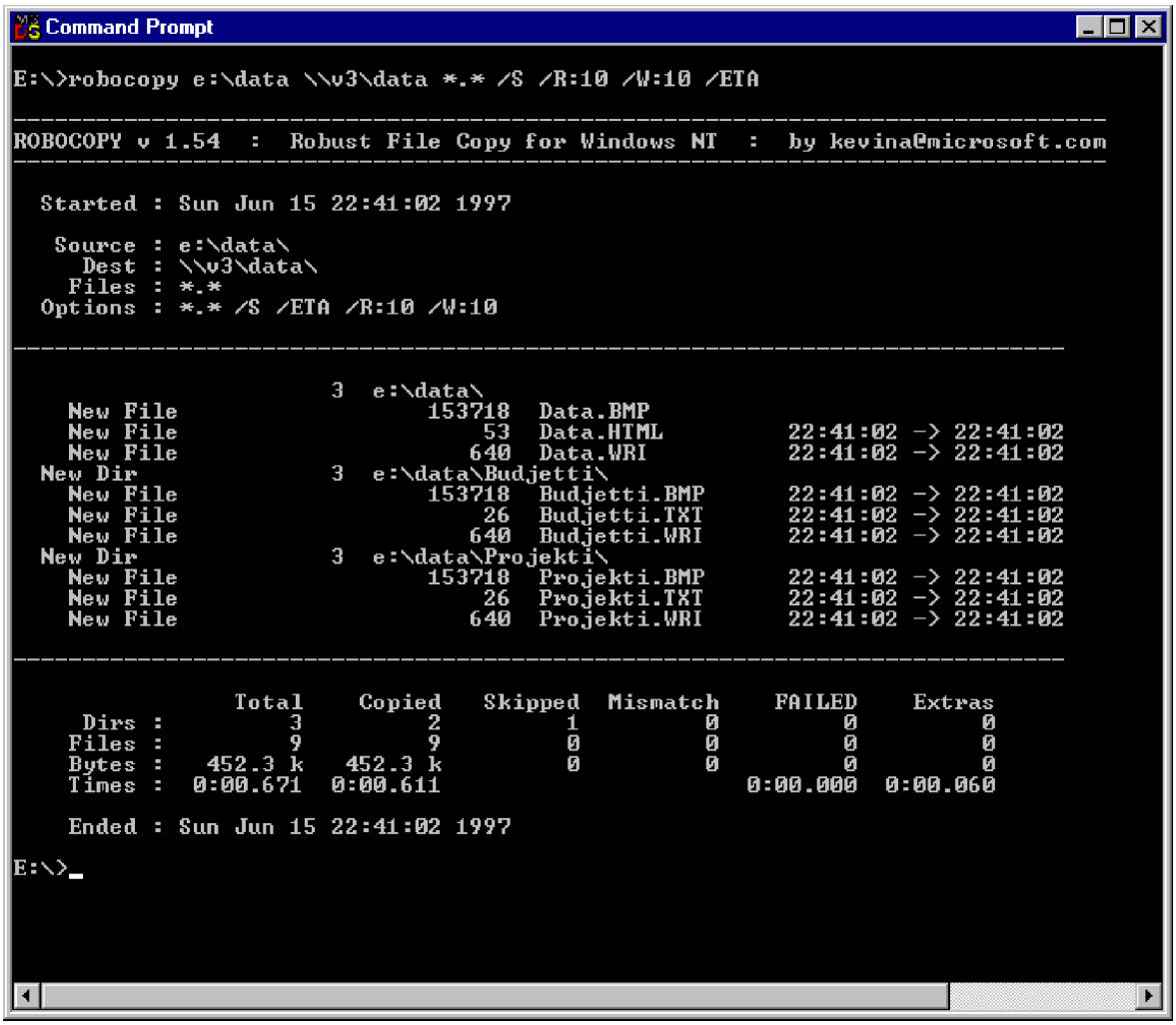
Tätä voi käyttää hyväksi toimittaessa ongelmallisen palvelimen kanssa.

ROBOCOPY

ROBOCOPY-apuohjelma on luotettava (*robust*) kopiointiohjelma NT-ympäristöön. Se mahdollistaa mm. Tiedostojen uudelleenkopiointiyritykset sekä odotusajan kopiointiyritysten välillä.

Esimerkiksi kopiointi paikallisen **E:\DATA**-hakemiston ja **V3**-palvelimen **DATA**-hakemiston välillä **10** uudelleenyrituksellä **10** sekunnin välein suoritetaan komennolla

```
ROBOCOPY  E:\DATA   \\V3\DATA  *.*  /S  /R:10  /W:10  /ETA
```

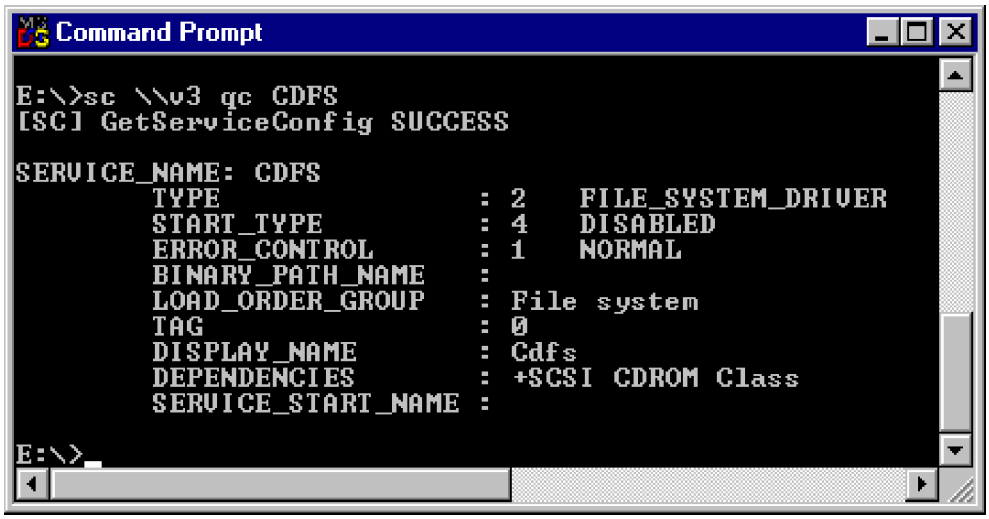


SC

SC on monipuolinen apuohjelma, jolla voi kysellä palveluiden konfigurointia, tilaa ja riippuvuuksia.

Ohjelma mahdollistaa myös konfiguroinnin muutokset, joita **ei** pidä tehdä ilman käsitystä siitä, mitä asetusten muutoksesta saattaa seurata.

Esimerkiksi **V3**-palvelimen **CDFS**-palvelun riippuvuudet:



Browser-palvelun **Services**-listassa näytettävä nimi:

SCLIST

SCLIST näyttää listauksen joko ajettavista tai pysäytetyistä palveluista.

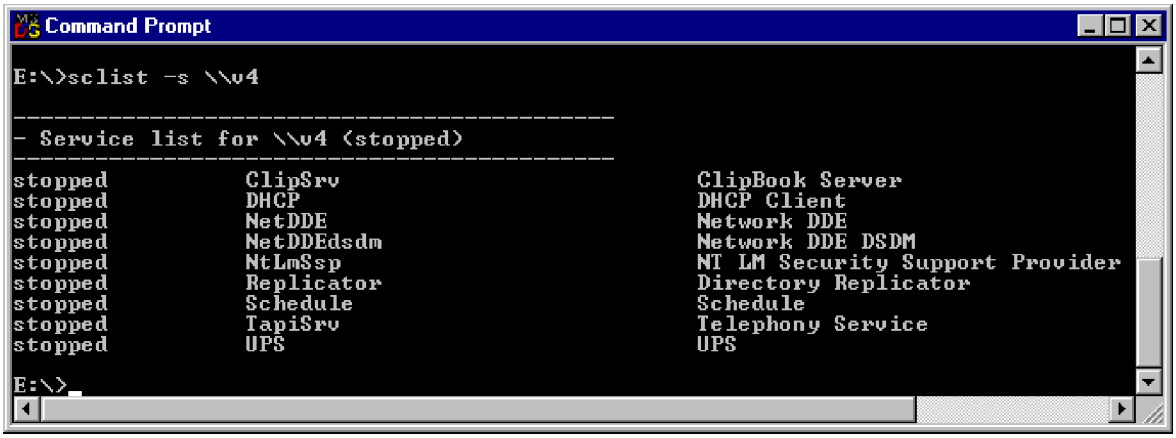
Syntaksi on:

SCLIST [-r] [-s] [NT-kone]

-r - näytetään vain ajettavat prosessit
-s - näytetään vain pysäytetyt prosessit

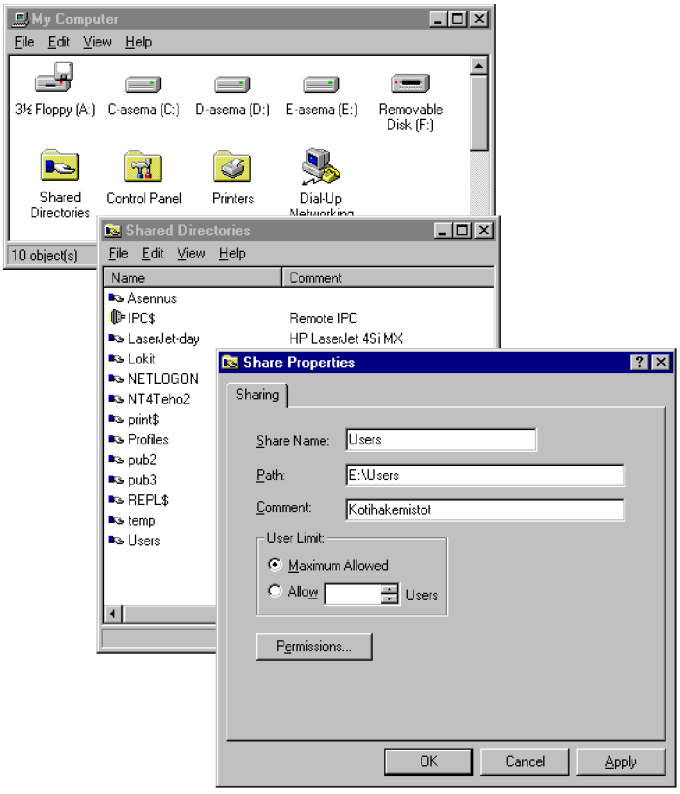
Esimerkiksi pysäytetyt prosessit **V4**-palvelimella saadaan komennolla

SCLIST -s \\V4



ShareUI

ShareUI -apuohjelma tuo **My Computer** -ikkunaan omana kuvakkeenaan jaetut kansiot, jonka avulla voidaan keskitetysti hallita palvelimesta jaettuja kansioita. Asennus tehdään etsimällä Resource Kitin hakemistosta **SHAREUI.INF** ja valitsemalla hiiren pikavalikosta **Install**.



Shutdown

SHUTDOWN on komentorivin komento, jolla voidaan ajaa alas paikallinen palvelin tai mikä tahansa verkon NT-kone.

Syntaksi on:

SHUTDOWN [\\NT-kone] [/L] [/A] [/R] [/T:xx] ["Sanoma"] [/Y] [/C]

Valitsimet ovat:

NT-kone - kohde
/L - kohteena paikallinen NT-kone
/A - alasajon keskeytys
/R - alasajon jälkeen uudelleenkäynnistys
/T:aika - odotusaika ennen alasajoa (oletus 20 sekuntia)
"**Sanoma**" - sanoma näyttöön
/Y - vastaa **Yes** kaikkiin kysymyksiin
/C - sulkee sovellukset antamatta mahdollisuutta tallennukseen.

Esimerkki:

Komentojono, joka tutkii, jos NT-koneessa ajetaan flipperiä. Jos ajetaan, se ajetaan alas ja käynnistetään uudelleen:

```
@ECHO OFF
RKILL /VIEW \\V3 > C:\T.TXT
FINDSTR "pinball PINBALL" C:\T.TXT > NUL
IF ERRORLEVEL 1 GOTO LOPPU
SHUTDOWN \\V3 /R /T:10 "Lopetetaanpas se Flipperin peluu!" /Y /C
:LOPPU
```

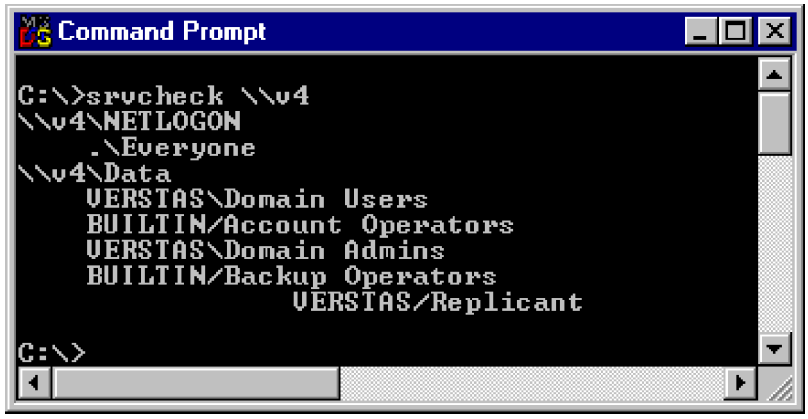
Apuna käytetään **Remote Kill**-palvelua.

Shutgui

SHUTGUI on Windows-versio **SHUTDOWN**-ohjelmasta. Resource Kitin **Shutdown Managerin** avulla voi sammuttaa (ja uudelleenkäynnistää) toisen NT-koneen ja aiemmissa NT-versioissa (ennen 4.0) tällä saattoi avata kohdekoneen näytönsäästäjän lukituksen!

SrvCheck

SRVCHECK-apuohjelma listaa kohteen jaetut resurssit sekä niiden oikeudet. Komento on **SRVCHECK \\palvelin**.



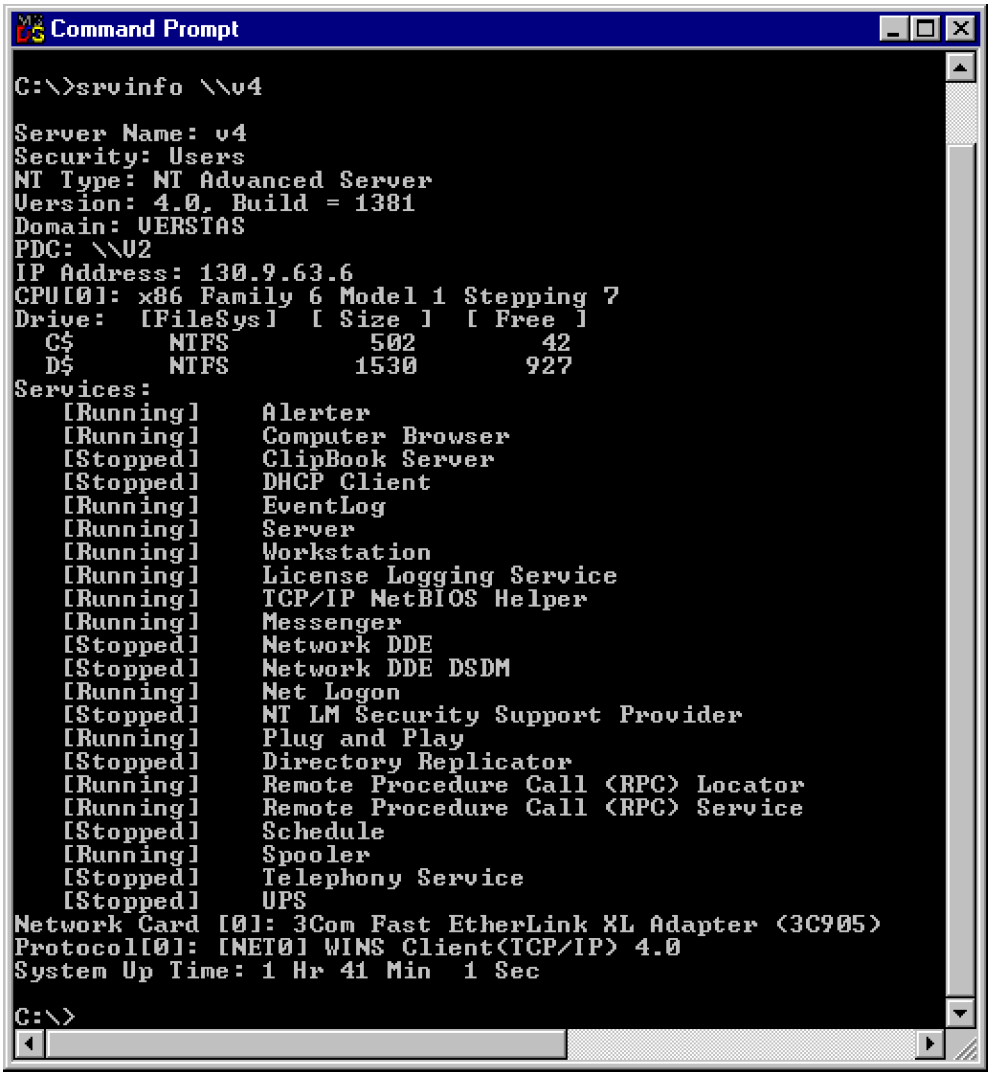
SrvInfo

SRVINFO on apuohjelma, joka kertoo yhteenvedon kohteen asetuksista. Syntaksi on:

SRVINFO [-ns|-d|-v|-s] \\NT-kone]

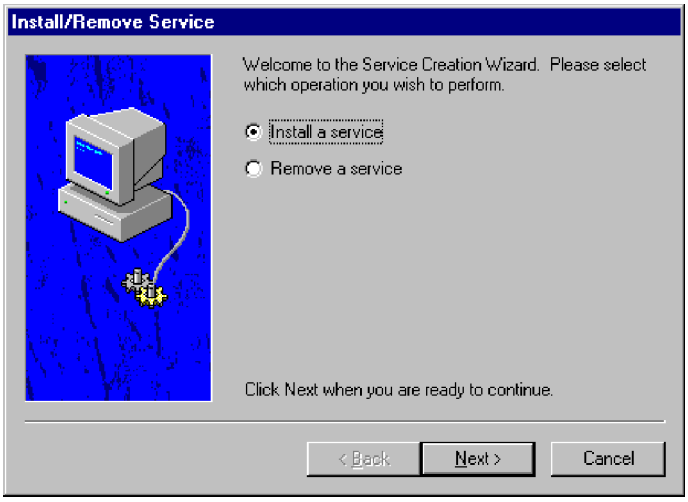
Valitsimet ovat:

-ns - ei palveluiden tietoja
-d - näytä palveluiden ja laiteohjainten tiedot
-v - versiotiedot Exchange- ja SQL Serveristä
-s - näytä jaot

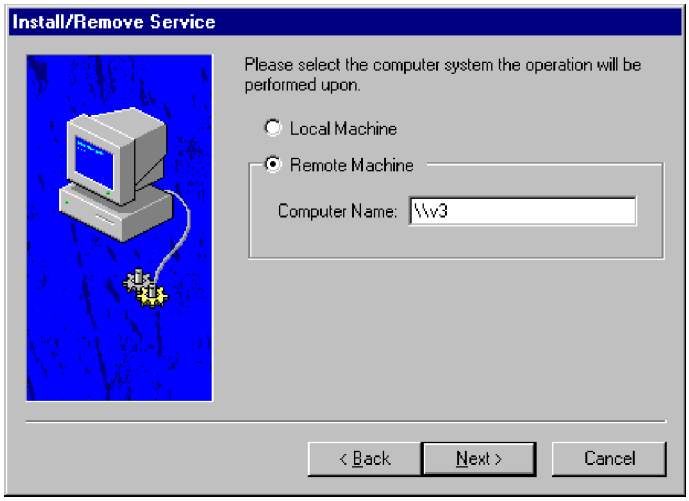


SRVINSTW

SRVINSTW on Windows-versio palveluiden asennusohjelmasta.



Voit jopa asentaa palvelun etäkoneeseen! Palvelun EXE-tiedoston on sijaittava kyseisen NT-koneen omalla kiintolevyllä.



TIMESERV

TIMESERV on apuohjelma, joka hakee kellonajan oman verkon ulkopuolisesta aikapalvelimesta. Kellonajan synkronointi oman verkon sisällä voidaan toteuttaa kirjauskomentojonoissa ajettavilla **NET TIME**-komennoilla, mutta jos halutaan käyttää ulkoista kellonaikaa tarjoavaa palvelinta, voidaan käyttää joko modeemi- tai internet-yhteyttä. **TIMESERV** tukee lisäksi GPS-korttia. Internet-aikaprotokollat ovat RFC 1305:n

mukainen **NTP** ja RFC 1769:n mukainen **SNTP**.

Aikapalvelun käyttöönotto tehdään seuraavasti:

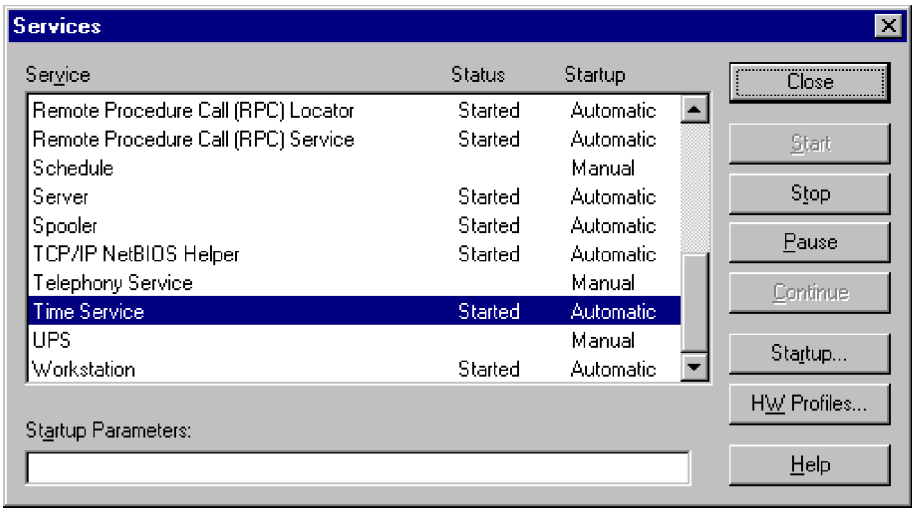
1) Kopioi **TIMESERV.DLL** ja **TIMESERV.EXE** %Systemroot%\System32-hakemistoon

2) Kopioi **TIMESERV.INI** %Systemroot%-hakemistoon

3) Editoi **TIMESERV.INI**:iä siten, että **NTPServer**-rivillä on joko NTP-palvelimen nimi tai IP-osoite. Selvitä tämä inetrnet-yhteyen tarjoajaltasi

4) Anna komento **TIMESERV -automatic**, mikä käynnistää aikapalvelun. Muut vaihtoehdot ovat **-manual** ja **-update**. **Update**-valintaa käytetään, jos olet muuttanut aikapalvelun asetuksia.

5) Käynnistä palvelu Ohjauspaneelissa **Services**-kuvakkeen avulla. Valitse **Time Service** ja paina **Start**.



Jos haluat asentaa lisäksi aikapalvelun työasemaan, voit toimia kuten edellä. Editoi kuitenkin **TIMESERV.INI**:ä siten, että siinä ovat asetukset:

Type=Primary
PrimarySource=\\palvelimesi

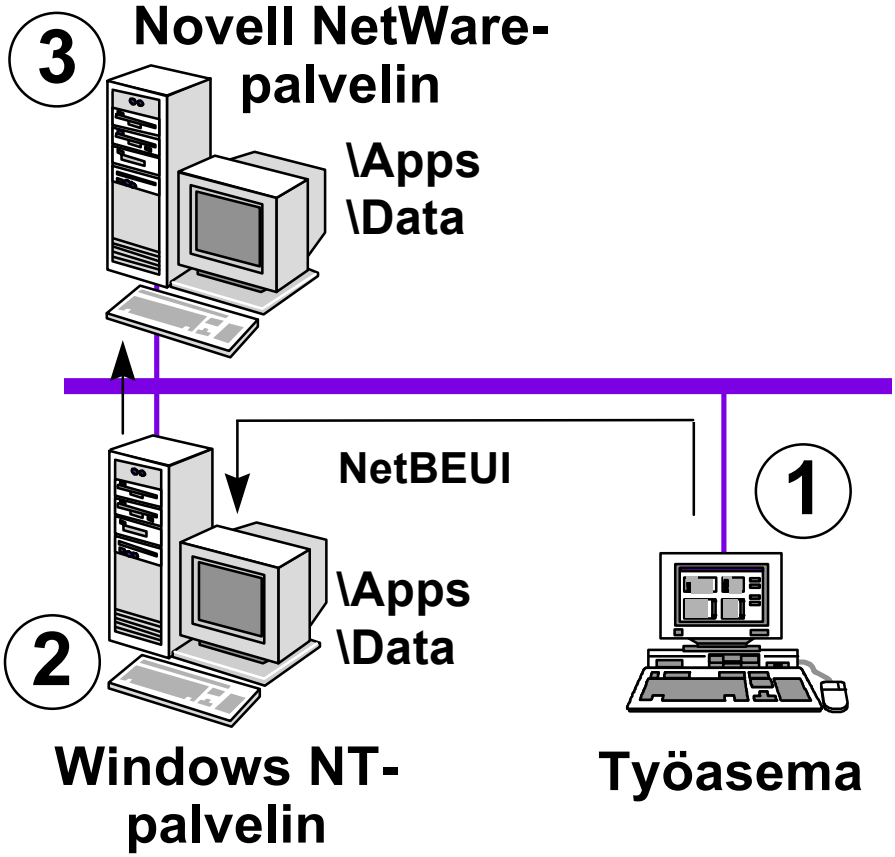
NetWare Compatible Gateway

Windows NT tukee Novell NetWare 2.15-, 3.x- ja 4.x-verkkoja. Pitkät tiedostonimetkin ovat käytettävissä, jos Novell NetWare -palvelimessa on ne otettu käyttöön OS/2:n varalta (*OS/2 Name Space*). Myös **NDS** (*Novell Directory Services*)-hakemistopalvelu on tuettu.

Windows NT-työasemassa tulee NetWare-asiakaspalvelu (Client Service for Netware) ja Windows NT-palvelimen mukana tulee NetWare-yhdyskäytäväpalvelu (Gateway Service for NetWare), jonka avulla NT-palvelin voi kytkeytyä Novell NetWare-palvelimeen ja jakaa sen resursseja - levyjakoja sekä kirjoittimia.

Yhdyskäytäpalvelun lisäksi palvelimessa tarvitaan lisäksi **NWLink IPX/SPX Compatible Transport**-protokolla.

Yhdyskäytävän periaate



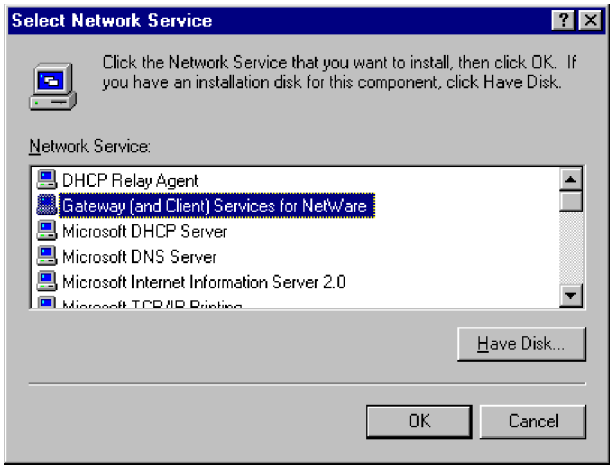
Työasema (**1**) kytkeytyy vaikkapa NetBEUI-protokollalla (muukin protokolla käy) NT-palvelimen jakamaan Novell NetWare-palvelimen resurssiin. NT-palvelin ohjaa resurssin käytön yhdyskäytävänsä kautta edelleen Novell NetWare-palvelimeen.

Käyttöönotto

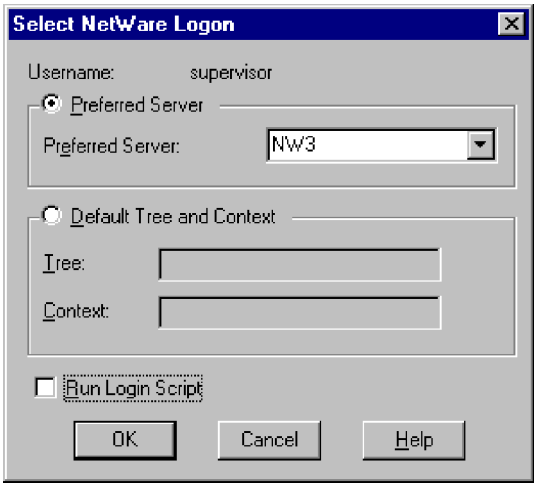
Yhdyskäytäpalvelun käyttöönotto tehdään seuraavasti:

1) Luo Novell-palvelimeen käyttäjäryhmä **NTGATEWAY**, johon lisäät käyttäjätunnuksen. Tämän käyttäjätunnuksen avulla yhdyskäytävä muodostuu

2) Asenna Windows NT -palvelimeen Ohjauspaneelin **Network**-kuvakkeen **Services**-välilehdellä **Add**-painikkeella palvelu **Gateway Service for NetWare**

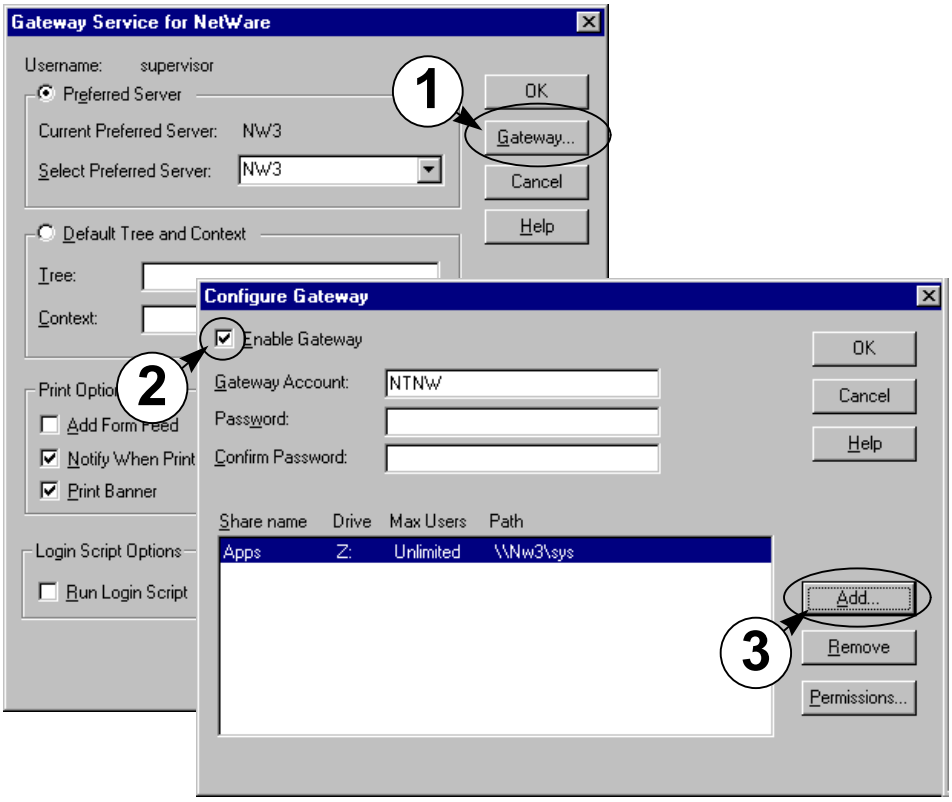


3) Käynnistä palvelin. Koska yhdyskäytävä toimii myös asiakkaana NetWare-verkoille, seuraavan kirjautumisen yhteydessä kysytään ensisijainen palvelin (**Preferred Server**), johon käyttäjä oletuksena kirjautuu.

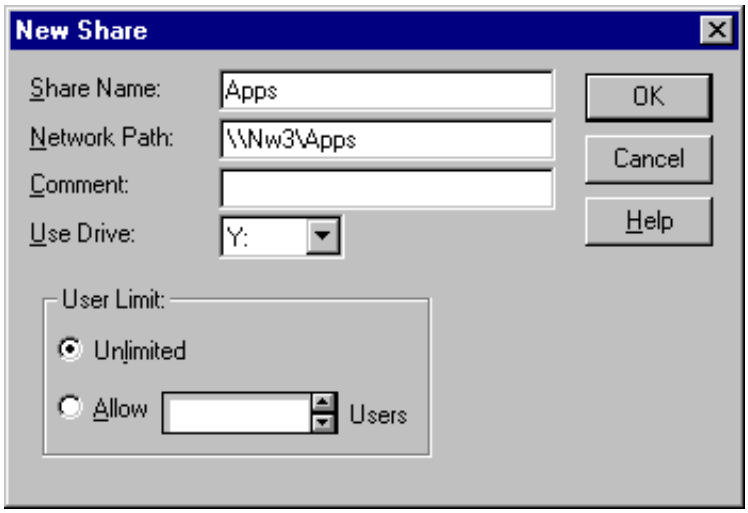


Asetukset

Ohjauspaneelin **GSNW**-kuvakkeella voidaan konfiguroida yhdyskäytävä. Valitse **Gateway**-painike (**1**), niin voit ottaa yhdyskäytävän käyttöön (**2**). Anna myös aiemmin lisäämäsi **NTGATEWAY**-ryhmän käyttäjätunnus salasanoineen. Tämän jälkeen voit **Add**-painikkeella lisätä NetWare-palvelimen jakamia resursseja.

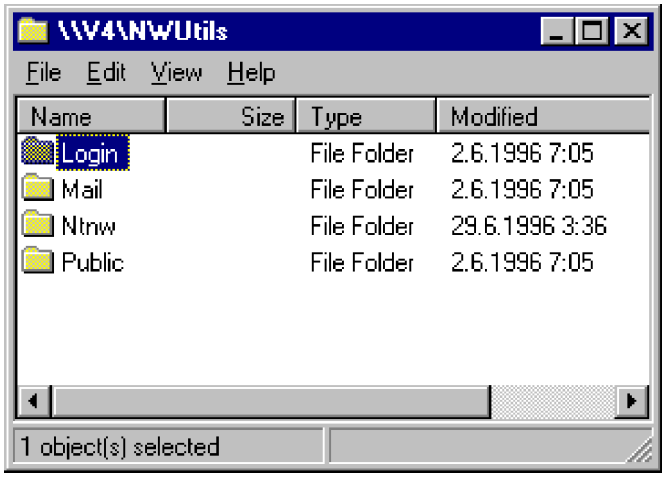


Voit antaa **Share Name**-kohtaan jakonimen, jolla resurssi näkyy NT-palvelimen kautta. **Network Path** on viittaus Novell-palvelimen jakamaan resurssiin. Anna myös levyasematunnus sekä käyttäjärajoitus.



Käyttäjäoikeuksia verkon kautta voit määritellä **Configure Gateway**-ikkunan **Permissions**-painikkeella.

Yhdyskäytävän jakamat resurssit näkyvät **My Computer**-ikkunassa. Työasemasta voidaan suoraan kytkeytyä jaettuun resurssiin.



Prosessien välinen kommunikointi

Sovelluksen suorittaminen jaetusti eri Windows NT-koneissa tulee yhä yleisemmäksi. Jaettujen sovellusten asiakas- ja palvelinosien välisen yhteyden täytyy mahdollistaa tiedon kulku molempiin suuntiin. Tämä yhteys voidaan muodostaa useilla tavoilla: Windows NT:ssä on seitsemän erilaista prosessien välistä tiedonsiirtomenetelmää:

- Named Pipes (nimetyt putket)
- Mailslots
- NetBIOS
- Windows Sockets
- Etäkutsupyynnöt (RPC:t)
- Network Dynamic Data Exchange (NetDDE)
- Server Message Blocks (SMB:t)
- Distributed Component Object Model (DCOM).

Named Pipes ja Mailslots

Putki on muistin osa, jonka kautta prosessi voi välittää tietoa toiselle prosessille. Putki yhdistää keskenään kaksi prosessia, jolloin yhden prosessin tulostetta voidaan käyttää toisen prosessin syötteenä.

Mailslot on yksisuuntainen kommunikointiväline, johon sovellus kirjoittaa sanoman ja toinen sovellus voi lukea sen. Ratkaisu soveltuu hyvin tiedon välittämiseen useammallekin vastaanottajalle. “Postilokero” on yksinkertainen ja väliaikainen tallennuspaikka palvelimen muistissa.

Nimetyt putket ja mailslotit kirjoitetaan itse asiassa tiedostojärjestelmäajureina, joten niiden käyttö poikkeaa muiden kommunikaatiomenetelmien käytöstä. Rekisterissä on asetukset NPFS:stä (*Named Pipe File System*) ja MSFS:stä (*Mailslot File System*). Koska ne ovat tiedostojärjestelmiä, niillä on muiden tiedostojärjestelmien kanssa yhteisiä toimintoja, esimerkiksi turvaominaisuuksia. Myös paikalliset

prosessit voivat käyttää nimettyjä putkia ja mailsloteja. Aivan kuin muissakin tiedostojärjestelmissä, etäkäyttö tapahtuu **uudelleenohjaimen** (*redirector*) kautta.

Nimetyt putket tarjoavat mahdollisuuden yhteysorientoituneeseen viestintään. Nimetyt putket perustuvat OS/2:n API-kutsuihin, jotka on liitetty Win32-pohjaisiin API-toimintoihin. Lisäksi on lisätty asynkroninen tuki, jotta nimetyt putket voisivat helpommin tukea asiakas/palvelinsovelluksia. Näiden OS/2:sta peräisin olevien API-toimintojen lisäksi Windows NT:ssä on erityisiä API-toimintoja, jotka parantavat nimettyjen putkien turvallisuutta.

Palvelin voi mm. muuttaa turvaidentiteettiään viestiä vastaanottavan asiakkaan määritysten mukaiseksi. Palvelimella on tavallisesti enemmän lupia palvelimen suojaustietokannan käyttöön kun asiakkaalla, joka pyytää palveluja. Kun pyyntö toimitetaan palvelimelle nimetyn putken kautta, palvelin muuttaa turvaidentiteettinsä asiakkaan ominaisuuksia vastaavaksi. Näin palvelimella käytössään on vain asiakkaan lupien verran oikeuksia, jolloin nimettyjen putkien turvallisuus paranee.

Windows NT -käyttöjärjestelmän mailslots -sovellus on osa Microsoft OS/2 LAN Manager -sovellusta. Windows NT -käyttöjärjestelmä käyttää kakkosluokan mailsloteja, jotka tarjoavat yhteydettömän viestinvälityksen viestien levitykseen. Viestin toimittaminen perille ei ole taattu, vaikkakin toimitusvarmuus on useimmissa verkoissa melko hyvä.

Yhteydetön viestinvälitys on käytännöllisintä verkon muiden tietokoneiden tai palvelujen tunnistamisessa, kuten esimerkiksi **selauspalvelussa** (Computer Browser).

NetBIOS

NetBIOS on standardiohjelmointirajapinta asiakas/palvelinsovellusten kehittämiseen PC-ympäristössä. NetBIOS:ia on käytetty rajapinnan prosessien välisenä kommunikaatiomenetelmänä 1980-luvun alusta alkaen.

NetBIOS- asiakas/palvelinsovellus voi kommunikoida useita eri protokollia käyttämällä:

- NetBEUI Frame -protokolla (NBF)
- NWLink NetBIOS (NWNBLink)
- NetBIOS TCP/IP:n kautta (NetBIOS over TCP/IP, NetBT). NetBT tarjoaa RFC 1001/1002 NetBIOS-tuen TCP/IP-protokollapinolle.

Ohjelmoinnin näkökulmasta korkeampitasoiset menetelmät (kuten nimetyt putket ja etäproseduurikutsut) ovat joustavampia.

NetBIOS käyttää seuraavia komponentteja:

- **Netapi32.dll** jakaa NetBIOS käyttäjätilassa ajettavan (*User-mode*) sovelluksen osoiteavaruuden (Netapi32.dll:ää käytetään myös muihin kuin NetBIOS-pyyntöihin.)
- **NetBIOS-emulaattori**, joka toimii NetBIOS-liitoskerroksena NetBIOS-sovelluksen ja TDI-sovellusten välissä.

MS-DOS- ja NetBIOS-sovellukset ohjelmoidaan käyttämään tiettyä LANA-numeroa verkkokommunikaatiossa. Kullekin verkkoreitille määritetään LANA-numero. Verkkoreitti koostuu protokolla-ajurista ja verkkosovittimesta, jota käytetään NetBIOS:in LANA-numerolleen lähettämiin komentoihin (katso tarkemmin NetBIOS Interface-palvelun konfiguroinnista aiemmin tässä luvussa).

Windows Sockets

Windows Sockets -API tarjoaa standardirajapinnan protokollille, joiden osoitekaaviot ovat erilaiset. Sockets-rajapinta kehitettiin Kalifornian yliopistossa Berkeleyssä 1980-luvun alussa. Windows Sockets API kehitettiin, jotta Sockets-rajapinta voitaisiin siirtää Windows- ja Windows NT -ympäristöihin. Windows Socketsin tarkoituksena oli myös osallistua API:n standardisoimiseen kaikille käyttöjärjestelmäalustoille. Windows Socketsia tukevat **TCP/IP**- ja **NWLink IPX/SPX**-protokollat.

Windows Sockets koostuu seuraavista komponenteista:

- **Wsock32.dll** jakaa Windows Socketsin käyttäjätilassa ajettavan (*User-mode*) sovelluksen osoiteavaruuden

- **Windows Sockets** -emulaattori, joka toimii Windows Sockets -liitoskerroksena Windows Sockets -sovellusten ja TDI:n mukaisten protokollien välissä.

Etäproseduurikutsut

Etäproseduurikutsujen (*Remote Procedure Call*, RPC) perustyöstä tehtiin suuri osa **Sun Microsystemsillä**. Työtä jatkoi **Open Software Foundation** (OSF) osana **Distributed Computing Environmentia** (DCE). Microsoftin RPC-sovellus on yhteensopiva OSF/DCE:n standardi-RPC:n kanssa, mutta Microsoft kehitti itse RPC:nsä alusta alkaen. RPC-menetelmä on täysin yhteensopiva muiden DCE-pohjaisten RPC-menetelmien kanssa (esimerkiksi Hewlett-Packardin HP-UX ja IBM:n AIX) ja sitä voidaan käyttää yhdessä niiden kanssa.

Microsoftin RPC-mekanismi on siinä mielessä ainutlaatuinen, että se muodostaa yhteyden asiakkaan ja palvelimen välillä muita prosessien välisiä kommunikaatiomenetelmiä käyttämällä. RPC voi käyttää kommunikaatioon etäjärjestelmien kanssa seuraavia menetelmiä:

- Nimetyt putket
- NetBIOS
- Windows Sockets.

Jos sovelluksen asiakas- ja palvelinosat ovat samalla koneella, tiedon siirtämiseen prosessien välillä voidaa käyttää paikallisia proseduurikutsuja (*Local Procedure Call*). Tästä syystä RPC on joustavin ja helpoimmin siirrettävä menetelmä prosessien väliseen kommunikaatioon.

RPC on menetelmä, jota tyypillisesti kannattaa käyttää asiakas/palvelinsovellusten kirjoittamiseen Windows NT :lle. Etäproseduurikutsun käyttämiseen tarvittavat komponentit kutsuvat seuraavia kohteita:

- **Remote Procedure Stub** (Proc Stub), joka paketoi palvelimelle lähetettävät etäproseduurikutsut RPC Run Timen avulla
- **RPC Run Time** (RPC RT), joka vastaa paikallisen ja etätietokoneen välisistä yhteyksista sekä välittää parametrit
- **Application Stub** (APP Stub), joka hyväksyy RPC RT:ltä tulevat etäkutsupyynnöt, purkaa paketin ja tekee tarvittavan kutsun etäproseduurille
- **Remote Procedure**, joka on verkon kutsuma varsinainen protokolla.

Network Dynamic Data Exchange

Network Dynamic Data Exchange (NetDDE) on Windowsin versiosta 2.x lähtien käytössä olleen dynaamisen tiedonsiirtoprotokollan (*Dynamic Data Exchange*, DDE) laajennus. NetDDE mahdollistaa DDE:n käytön NetBIOS-yhteensopivan verkon yli.

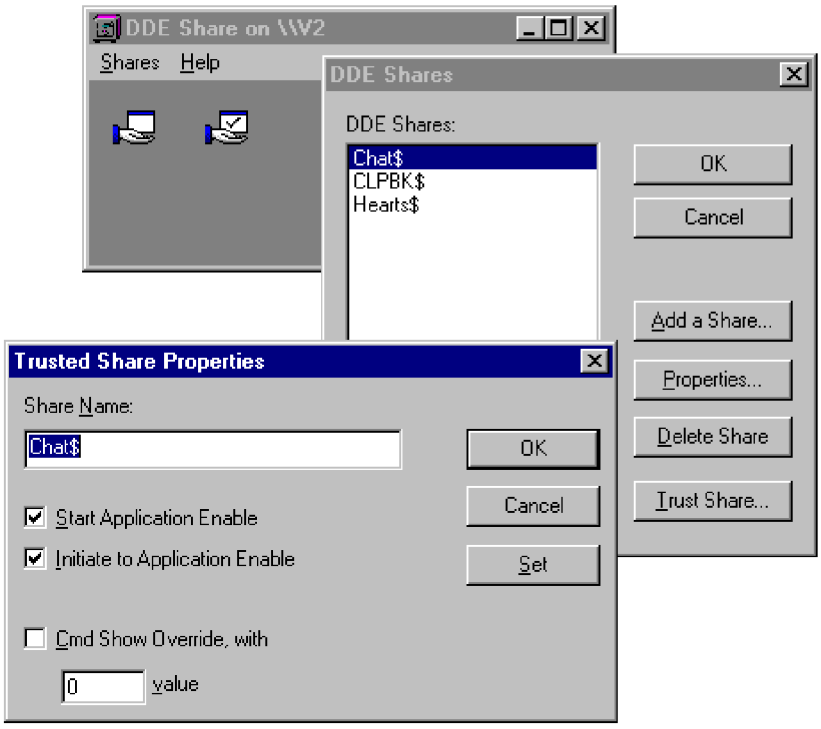
DDE puolestaan on protokolla, jonka avulla sovellukset voivat vaihtaa tietoja. Tämän vaihdon tekemiseksi protokollien täytyy ensin käynnistää DDE-keskustelu. DDE-keskustelun aloittava sovellus on DDE-**asiakassovellus**, ja pyyntöön vastaava sovellus on **DDE-palvelinsovellus**.

Yksi sovellus voi osallistua samanaikaisesti useisiin DDE-keskusteluihin ja toimia joissakin keskusteluissa DDE-asiakassovelluksena ja toisissa keskusteluissa DDE-palvelinsovelluksena. Näin käyttäjä voi luoda sovellusten välille DDE-linkin ja antaa yhden sovelluksen päivittää toista automaattisesti.

NetDDE laajentaa DDE:n ominaisuudet verkkokäyttöön NetBIOS-emulaattorin avulla. Näin kahdella tai useammalla työasemalla olevat sovellukset voivat jakaa tietoa dynaamisesti keskenään. NetDDE ei ole DDE:n erikoismuoto, vaan pikemminkin palvelu, joka tutkii DDE-keskusteluun sisältyviä tietoja ja etsii erityistä sovellusnimeä. NetDDE:n käyttö tällä tavoin mahdollistaa NetDDE:n käytön DDE-sovelluksille ilman muutoksia.

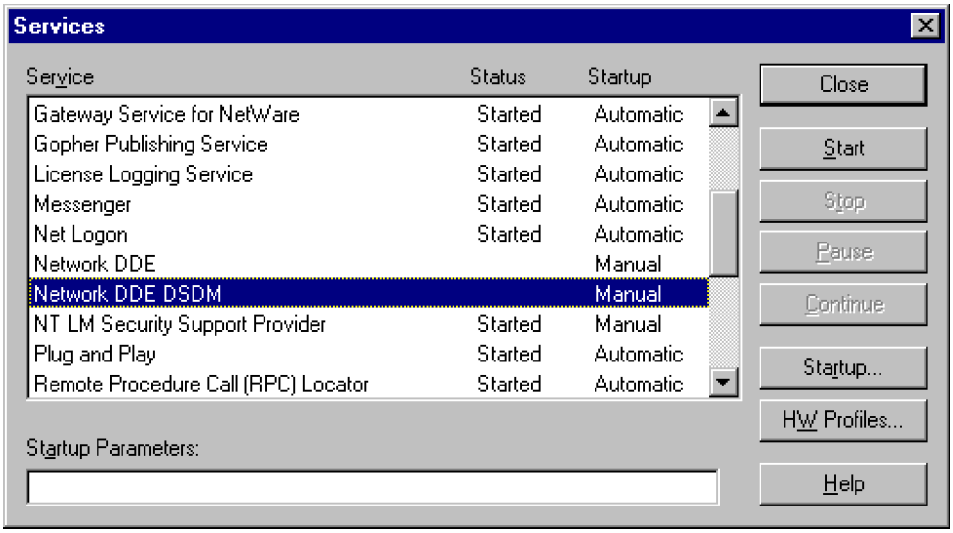
NetDDE-palvelu tutkii DDE-pyynnön ja etsii tiettyä NetDDE:n käyttöön varattua sovellusnimeä, jonka edessä on etäjärjestelmän nimi. Varattu sovellusnimi on NDDE$, ja NetDDE etsii DDE-pyyntöä, joka käyttää sovellusnimeä muodossa **<palvelinnimi>****ndde$**.

Ennen kuin käyttäjä voi ottaa yhteyden etäkoneella sijaitsevaan kirjoittimeen tai hakemistoon, kirjoitin tai hakemisto täytyy jakaa. Tietokoneelle täytyy samoin luoda NetDDE, ennen kuin sillä oleva sovellus voi käyttää NetDDE:tä kommunikaatioon toisella tietokoneella olevan sovelluksen kanssa. NetDDE:n tunnistavat sovellukset (kuten **Chat**) luovat automaattisesti NetDDE-osion asennusvaiheessa. Muille sovelluksille täytyy luoda NetDDE-osio ClipBook Viewerillä, jolloin tietoa voidaan vaihtaa leikepöydän kautta. Windows NT:n mukana tulevan DDE Share -apuohjelman (**DDESHARE.EXE**) avulla voidaan määrittää NetDDE-osio, jolloin sovellukset voivat vaihtaa tietoa suoraan.



NetDDE-osiot määritetään rekisterissä. Niitä käytetään kommunikoimalla **Network DDE Service Data Managerin** (DSDM) kanssa, joka on NetDDE:tä tukeva Windows NT -käyttöjärjestelmän palvelu. Koska NetDDE on DDE:n laajennus, NetDDE-keskustelujen muodostamiseen käytetään samoja API-toimintoja kuin DDE-keskusteluissakin.

Windows NT 3.1:ssä ladataan NetDDE-palvelut automaattisesti käynnistysvaiheessa. Windows NT 3.5:ssä ja uudemmissa versioissa NetDDE:n oletuskäynnistystyyppi on manuaalinen, jolloin käynnistys on nopeampaa. NetDDE-palvelujen käynnistystyyppi voidaan konfiguroida Ohjauspaneelin kautta.



Server Message Blocks

Server Message Blocks (SMB) -protokollan ovat kehittäneet yhdessä Microsoft, Intel ja IBM. Siinä määritetään komennot, joiden avulla välitetään tietoa verkon tietokoneiden välillä. **Uudelleenohjain** (*Redirector*) paketoi etätietokoneille tarkoitetut **Network Control Block** (NCB) -pyynnöt SMB-rakenteeseen. Se käyttää myös SMB:tä pyyntöjen tekemiseen paikallisen tietokoneen protokollapinolle, kuten esimerkiksi ”luo istunto tiedostopalvelimeen”.

SMB käyttää neljää viestityyppiä:

- Istunnonhallintaviestit (*Session control message*), jotka koostuvat uudelleenohjaimen yhteyden palvelimen jaettuun resurssiin aloittavista ja lopettavista komennoista
- Tiedostoviestit (*File message*), joita uudelleenohjain käyttää pääsyyn palvelimella oleviin tiedostoihin
- Kirjoitinviestit (*Printer message*), joita uudelleenohjain käyttää datan lähettämiseen palvelimen tulostusjonoon ja tulostusjonon tilatietojen hakemiseen
- Viestiviestit (*Message message*), joiden avulla sovellus voi vaihtaa viestejä toisen työaseman kanssa.

SMB:t mahdollistavat yhteistoiminnan Microsoft-verkkotuotteiden eri versioiden välillä ja esimerkiksi seuraaviin SMB:itä käyttäviin verkkoihin:

- MS OS/2 LAN Manager
- Työryhmä-Windows
- IBM LAN Server
- MS-DOS LAN Manager
- DEC PATHWORKS
- Microsoft LAN Manager for UNIX
- 3Com 3+Open
- MS-Net.

Distributed Component Object Model

Windows NT Server tukee nyt paikallisen tietokoneen prosessien välisen viestinnän mahdollistavan COM:in (*Component Object Model*) lisäksi myös DCOM:ia (*Distributed Component Object Model*, jaettu COM). DCOM (tai verkko-OLE) mahdollistaa prosessien tehokkaan jakamisen eri tietokoneille, jolloin sovelluksen asiakas- ja palvelinkomponentit voidaan sijoittaa verkossa sopivimpiin paikkoihin. Käsittely tapahtuu käyttäjän kannalta läpinäkyvästi - käyttäjä voi käyttää ja jakaa tietoja ilman, että hänen tarvitsee tietää, missä sovelluskomponentit ovat. Jos sovelluksen asiakas- ja palvelinkomponentit sijaitsevat samalla

tietokoneella, tietoa voidaan siirtää prosessien välillä DCOM:in avulla. DCOM on alustariippumaton ja tukee 32-bittisiä sovelluksia, jotka tunnistavat DCOM:in.

Sovelluksen ominaisuudet täytyy määrittää **DCOM Configuration**-ohjelmalla ennen kuin sovellusta voidaan käyttää DCOM:in avulla.

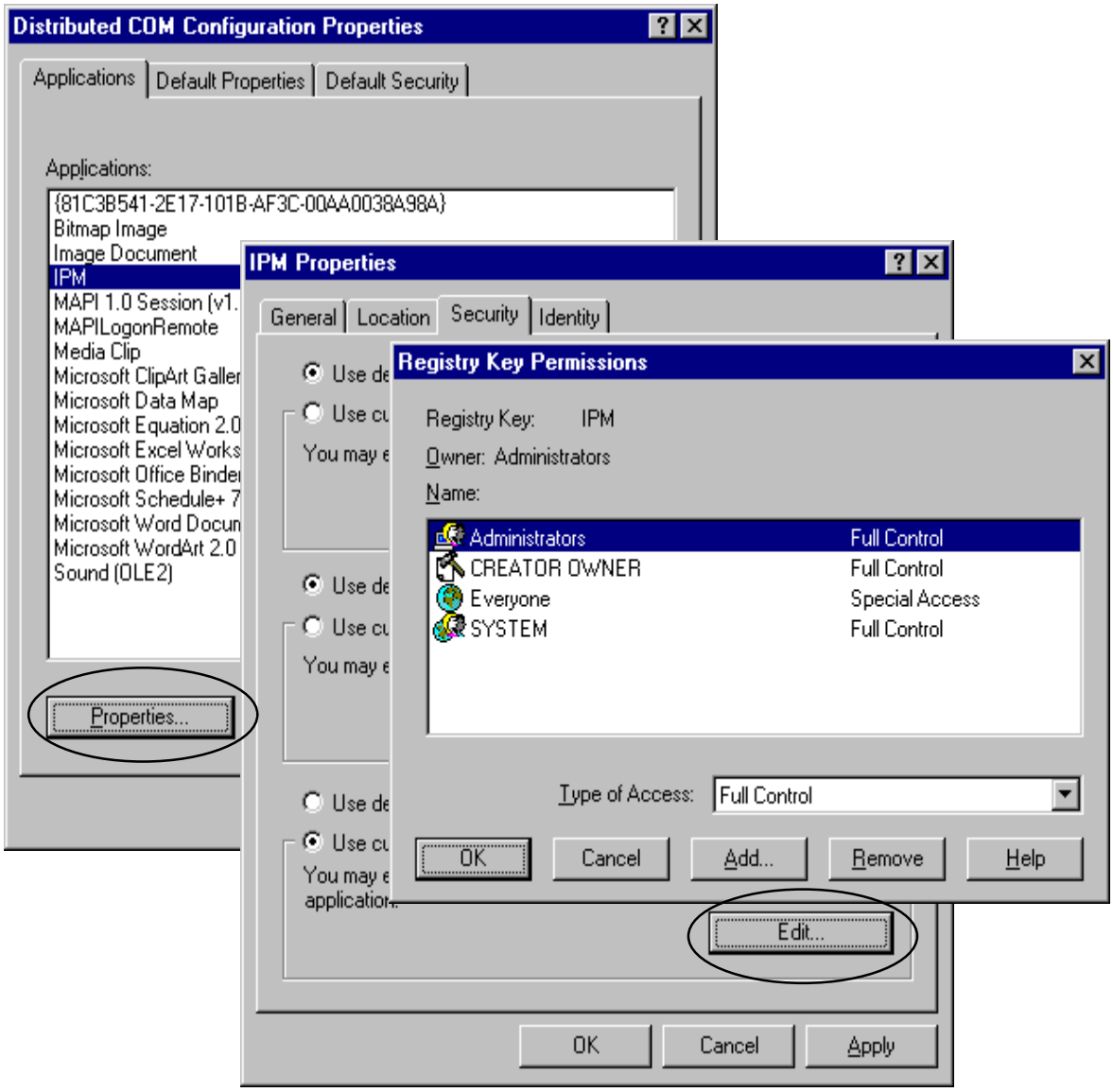
DCOM:in etuja

DCOM on sopiva menetelmä kehittäjille, kun kirjoitetaan asiakas/palvelinsovelluksia Windows NT:lle. Ainoastaan käyttöjärjestelmän tarvitsee tietää, käsitelläänkö kutsuttavaa funktiota samassa prosessissa vai verkon kautta. Sovelluksen ei tarvitse välittää paikallisista tai etäkutsupyynnöistä. Verkon pääkäyttäjät voivat valita DCOM-sovellukset käytettäviksi paikallisilla tai etätietokoneilla ja tasapainottaa kuormitusta konfiguraatiota muuttamalla.

DCOM käyttää etäkutsumenettelyä (RPC) tarjotakseen laajennettavan ja helppokäyttöisen mekanismin jaettujen sovellusten integroimiseen verkossa. Jaettu sovellus koostuu useista prosesseista, jotka yhdessä suorittavat jonkin yksittäisen tehtävän. Toisin kuin muut prosessien väliset kommunikaatiomenetelmät, DCOM antaa käyttäjälle hyvät mahdollisuudet valvoa turvaominaisuuksia (kuten käyttöoikeuksia). Sen avulla voidaan myös käynnistää sovelluksia muilla tietokoneilla ja integroida WWW-pohjaisia sovelluksia, joita ajetaan **ActiveX**-alustalla.

DCOM:in konfigurointi

Windows NT 4.0:n turvaominaisuudet voidaan helposti ulottaa DCOM-objekteihin. Pääkäyttäjät määrittävät DCOM-sovellusten luvat, jotka voivat olla erilaiset paikalliseen ja etäkäyttöön.



Kun DCOM:ia käyttävä sovellus on asennettu, voidaan käyttää DCOM Configurationia (**DCOMCNFG.EXE**) seuraaviin tehtäviin:

- DCOM:in käytön estäminen, jotta sitä ei voida käyttää tietylle tietokoneelle tai sovellukselle

- Sovelluksen sijainnin määrittäminen

- Palvelinsovelluksen ominaisuuksien asettaminen määrittämällä, millä käyttäjätunnuksilla se voidaan tai ei voida käynnistää. Voit myöntää lupia, jotka pätevät joko kaikkiin tietokoneelle asennettuihin sovelluksiin tai vain tiettyyn sovellukseen

- Palvelinsovelluksen ajamiseen käytettävän käyttäjätunnuksen määrittäminen. Asiakassovellus käynnistää tällä tunnuksella

prosesseja ja käyttää toisilla toimialueen koneilla olevia resursseja. Jos palvelinsovellus on asennettu palveluna, sovellus voidaan ajaa System-käyttäjätunnuksella tai itse luodulla Windows NT Server-palvelutunnuksella

- Tietoturvallisuuden tason valvomiseen (esimerkiksi pakettien salakirjoittaminen) sovellusten välisissä yhteyksissä.

Sekä asiakassovellusta että palvelinsovellusta ajavien tietokoneiden täytyy olla konfiguroituja käyttämään DCOM:ia. Asiakkaana toimivalle tietokoneelle täytyy määrittää käytettävän tai käynnistettävän palvelinsovelluksen sijainti. Palvelimena toimivalle koneelle täytyy määrittää käyttäjätunnus, jolla on oikeus käynnistää tai käyttää sovellusta sekä käyttäjätunnus, jota käytetään sovelluksen ajamiseen.

8. TCP/IP

TCP/IP on reitittävä protokolla, joka koostuu Internet-protokollista. Ne standardoivat, kuinka tietokoneiden välillä siirretään tietoa, kuinka verkot kytketään ja kuinka reititys hoidetaan verkossa. TCP/IP-lyhenne koostuu kahdesta eri osasta: **TCP** (*Transmission Control Protocol*) ja **IP** (*Internet Protocol*). TCP/IP:n **ydinprotokollat** ovat seuraavat:

- TCP (Transmission Control Protocol)
- IP (Internet Protocol)
- UDP (User Datagram Protocol)
- ARP (Address Resolution Protocol)
- ICMP (Internet Control Message Protocol)

Tyypillisiä TCP/IP-**sovelluspalveluita** ovat esimerkiksi seuraavat:

- FTP (*File Transfer Protocol*)
- SMTP (*Simple Mail Transfer Protocol*)
- SNMP (*Simple Network Management Protocol*)

TCP/IP:n perusteita on käsitelty laajemmin **Windows NT 4.0 Tehokäyttäjän Opas 1**:ssä.

Internet Architecture Board (IAB) on **Internet Societyn** (**http://www.isoc.org**) tekninen elin, jonka tutkijoista, suunnittelijoista ja operaattoreista koostuva **Internet Engineering Task Force** (IETF) työryhmä standardoi Internetin protokollia. Määritykset on julkaistu **Request for Comments** (RFC)-dokumentteina. Näihin dokumentteihin viitataan toisinaan tässä luvussa. **InterNIC** löytyy osoitteesta **http://www.internic.net**.

IP-protokolla

IP (*Internet Protocol*) on TCP/IP-pinon jakelukeskus, jossa pakettien lajittelu ja jakelu tapahtuu. Tässä kerroksessa jokainen saapuva ja lähtevä paketti tunnetaan nimellä **tietosähke** (datagram). Kukin IP-datagrammi sisältää lähettäjänsä IP-osoitteen sekä aiotun vastaanottajan IP-osoitteen. Toisin kuin **MAC-osoitteet** (esimerkiksi verkkokortin laiteosoite), tietosähkeen IP-osoitteet pysyvät samoina koko matkan.

ARP

Lähiverkossa liikennöinnin edellytys on se, että solmut tietävät toistensa IP- ja MAC-osoitteet. Koska MAC- ja IP-osoitteen välillä ei ole mitään yhteyttä, voidaan käyttää kahta ratkaisua: käytetään joko kiinteää kuvausta, jossa yhteydet määritellään, tai menettelyä, jolla voidaan fyysinen osoite yhdistää IP-osoitteeseen.

Jälkimmäinen on **ARP**:n (*Address Resolution Protocol*) tehtävä - hoitaa fyysisen- ja IP-osoitteen yhdistäminen eli ARP sovittaa IP:n allaolevaan verkkoon.

ARP-protokollaa joudutaan käyttämään tilanteessa jossa solmu haluaa lähettää, mutta sen tiedossa on ainoastaan vastaanottajan IP-osoite. Tällöin lähettäjä generoi **ARP-kyselyn** ja lähettää sen verkkoon. Kysely on tyypiltään broadcast- eli yleissanoma (levitysviesti), joka menee kaikille kyseessä olevan segmentin asemille. Sanoma sisältää IP-osoitetiedot lähettäjästä ja vastaanottajasta sekä lähettäjän MAC-osoitteesta. Kaikki asemat sijoittavat lähettäjän IP- ja MAC-osoitetiedot omaan ARP-tauluun ja vastaanottajaksi merkitty asema täyttää sanomasta kohdan "vastaanottajan MAC-osoite" sekä palauttaa sanoman takaisin lähettäjälle. Lähettäjä vastaanottaa sanoman ja merkitsee saadun MAC-osoitteen omaan ARP-tauluun. Tämän jälkeen lähetys onnistuu.

RARP (*Reverse ARP*) hoitaa lähes samoja tehtäviä kuin ARP, mutta toiseen suuntaan. RARP vastuulla on selvittää tietokoneelle sen oma IP-osoite. Tätä protokollaa tarvitaan etenkin sellaisessa tilanteessa, jossa solmulla itsessään ei ole tallennuskapasiteettia IP-osoitteen tallennusta varten.

IP-osoite

Jotta TCP/IP-protokollaa voitaisiin käyttää, tietokoneessa tarvitaan verkko- ja isäntätunnus. Vaikka itse IP-osoite on **yksi luku**, se sisältää kaksi tunnusta: **verkkotunnuksen** ja kyseisen tietokoneen **isäntätunnuksen**. Isäntä eli *host* voi tässä yhteydessä tarkoittaa mitä tahansa verkkoon kytkettyä laitetta, joka käyttää TCP/IP-protokollaa. Samaan **loogiseen verkkoon** kuuluvilla tietokoneilla ja verkkoon kytketyillä oheislaitteilla on sama verkkotunnus.
Lähiverkkoja yhdistävissä verkoissa vastaavasti kullakin lähiverkolla on oma tunnus. Isäntätunnusta käytetään verkon yksittäisten tietokoneiden tunnistamiseen.

Isäntätunnus

Internet-osoitteet on jaettu osoiteluokkiin, joita käytetään eri kokoisissa verkoissa. Osoiteluokka selviää **IP-osoitteen ensimmäisestä numerosarjasta**. Alla olevassa taulukossa on yhteenveto osoiteluokista ja niissä käytettävistä verkko- ja isäntätunnuksista sekä kussakin luokassa käytettävissä olevien verkko- ja isäntätunnusten enimmäismäärä:

Luokka	Verkkoja	Laitetta/ verkko	Verkkotunnukset	Aliverkon peite
A	126	167.772.214	1.0.0.0- 126.0.0.0	255.0.0.0
B	16.384	65.534	128.1.0.0- 191.254.0.0	255.255.0.0
C	2.097.151	254	192.0.1.0- 223.255.254.0	255.255.255.0

Isäntätunnuksia **0** ja **255** ei pidä käyttää tietokoneiden tunnuksina, vaan niitä käytetään tavallisesti yleislähetysosoitteina (*broadcast address*), joille lähetetyt paketit kaikki isännät ottavat vastaan.

Aliverkko

Verkkosolmu käyttää **verkko-** ja **isäntätunnuksia** päättäessään, ottaako se paketin vastaan, sekä määrittäessään lähetysten laajuuden. Solmut vastaanottavat IP-lähetyksiä vain solmuilta, joilla on sama verkkotunnus. Koska jokaisessa IP-paketissa on lähettäjän IP-osoite, vastaanottavan solmun tulee erottaa IP-osoitekentästä **lähdeverkon** ja **-isännän tunnukset**. Erottelu tehdään **aliverkon peitteen** eli **verkkomaskin** (*Subnet Mask*) avulla, joka on **32-bittinen** arvo. Kuten IP-osoitekin, aliverkon peite esitetään yleensä pisteillä erotettuina kymmenjärjestelmän lukuina, esimerkiksi **255.255.0.0**. Aliverkon peite määritetään asettamalla **verkkotunnukseen kuuluvien bittien arvoksi 1** ja **isäntätunnukseen kuuluvien bittien arvoksi 0**. Tämän jälkeen peite muunnetaan pisteillä erotetuiksi kymmenjärjestelmän luvuiksi seuraavasti:

Osoite	Aliverkon peite (binaarimuoto)	Aliverkon peite
A-luokka	11111111 00000000 00000000 00000000	255.0.0.0
B-luokka	11111111 11111111 00000000 00000000	255.255.0.0
C-luokka	11111111 11111111 11111111 00000000	255.255.255.0

Saadun tuloksen avulla TCP/IP voi määrittää tietokoneen verkko- ja isäntätunnuksen. Jos IP-osoite on esimerkiksi **128.211.88.9** ja aliverkon peite on **255.255.0.0**, verkkotunnus on **128.211** ja isäntätunnus **88.9**.

Kaikkien samaan fyysiseen verkkoon liitettyjen komponenttien on syytä käyttää samaa verkkotunnusta ja aliverkon peitetä, muuten seuraa osoitus- ja reititysongelmia.

Esimerkkinä B-luokan aliverkon peitteet:

Aliverkkojen lkm	Isäntäkoneita aliverkossa	Bittien lkm	Aliverkon peite
0	-	1	-
2	16382	2	255.255.192.0
6	8190	3	255.255.224.0
14	4094	4	255.255.240.0
30	2046	5	255.255.248.0
62	1022	6	255.255.252.0
126	510	7	255.255.254.0
254	254	8	255.255.255.0

Windows NT -koneessa IP-osoite annetaan **IP-osoite** (IP Address)-välilehdessä antamalla IP-osoite ja aliverkon peite. Voit myös käyttää DHCP-palvelua hyväksesi valitsemalla **Hae IP-osoite DHCP-palvelimelta** (Obtain an IP address from DHCP server). Palvelimissa näin ei yleensä tehdä.

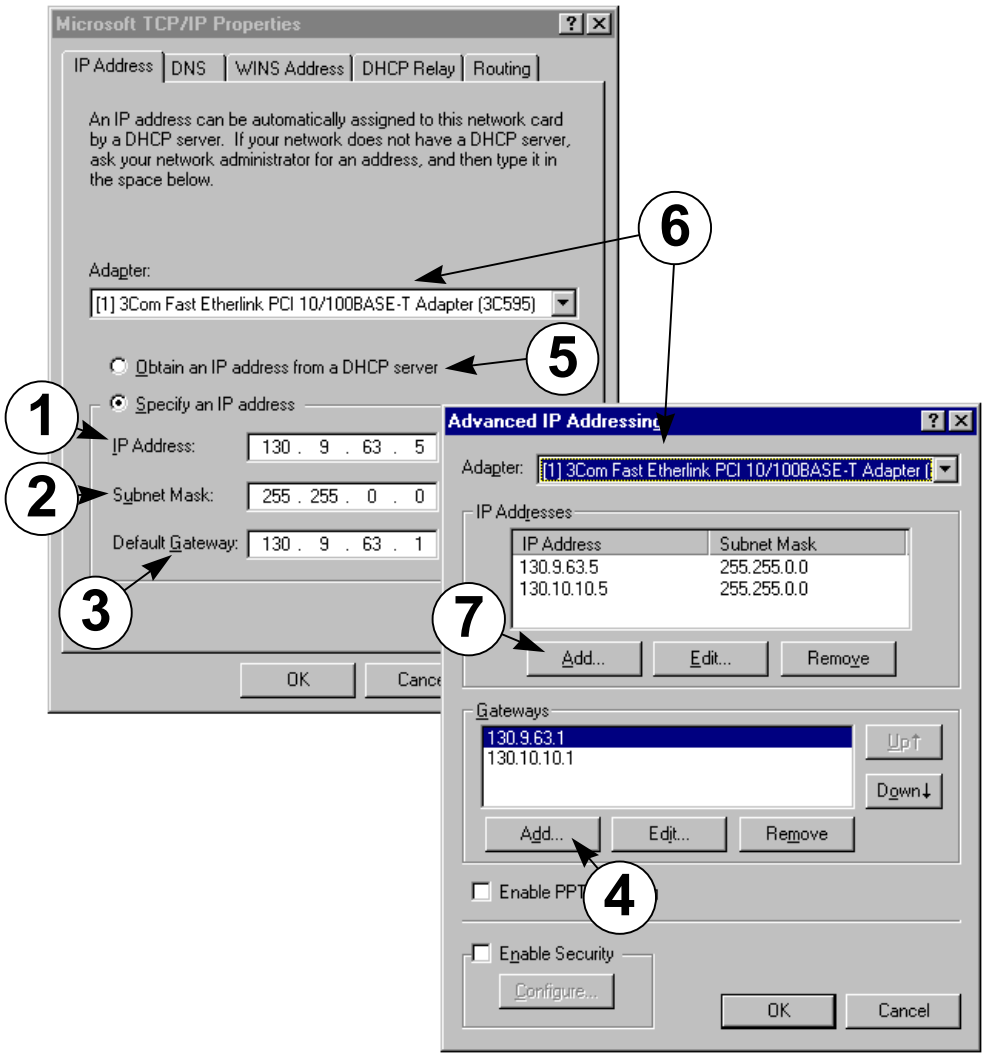
IP-osoiteasetukset Windows NT:ssä

Windows NT -koneessa IP-osoite annetaan kohdassa **IP Address** (**1**) ja aliverkon peitto kohdassa **Subnet Mask** (**2**). **Oletusyhdyskäytävä** annetaan **IP Address**-välilehdessä kohtaan **Default Gateway** (**3**).

Advanced IP Addressing-välilehdessä painikkeella **Add** voit lisätä useampia yhdyskäytäviä (**4**) ja määritellä niiden käyttöjärjestyksen.

Voit myös käyttää DHCP-palvelua hyväksesi valitsemalla **Hae IP-osoite DHCP-palvelimelta** (Obtain an IP address from DHCP server)(**5**). Paikalliset asetukset kuitenkin ohittavat DHCP-palvelimen antamat asetukset. Palvelimissa näin ei yleensä tehdä.

Jos NT-koneessa on useampia verkkokortteja (*multihoming*), niin voit määritellä asetukset verkkokorttikohtaisesti (**6**). Voit myös määritellään yhteen tai useampaan verkkokorttiin yhden tai useamman IP-osoitteen (**7**).



Reititys

Reititys (*Routing*) on IP:n ensisijainen tarkoitus. IP-protokolla saa tietosähkeet yläkerroksista UDP- ja TCP-protokollilta sekä alakerroksesta verkkokortilta. Jokaisessa tietosähkeessä on lähettäjän ja vastaanottajan IP-osoitteet. IP-protokolla tutkii kohdeosoitteen, vertaa sitä paikalliseen **reititystauluun** (*Route table*) ja päättää vertailun perusteella, mitä tietosähkeelle pitää tehdä. Mahdollisuuksia on kolme:

- Paketti voidaan välittää ylöspäin jollekin paikallisen tietokoneen IP-protokollan yläpuolella olevalle protokollalle
- Paketti voidaan välittää eteenpäin käyttäen jotakin paikallista verkkokorttia
- Paketti voidaan hylätä.

Reititystaulu

Reititystaulussa on neljäntyyppisiä reittejä. Ne on lueteltu alla siinä järjestyksessä, jossa IP-protokolla vertaa paketin tietoja reititystaulukkoon:

- **Isäntäkone** (*Host*) - reitti yksittäiseen tietokoneeseen, tiettyyn IP-osoitteeseen
- **Aliverkko** (*Subnet*) - reitti aliverkkoon
- **Verkko** (*Network*) - reitti kokonaiseen verkkoon
- **Oletus**, jota käytetään, ellei mikään vaihtoehdoista 1-3 täsmää.

Voit tarkastella NT-koneen reititystaulua komennolla **ROUTE PRINT:**

Rivi	Network Address	Netmask	Gateway Address	Interface	Metric
1	0.0.0.0	0.0.0.0	130.9.63.1	130.9.63.5	1
2	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
3	130.9.0.0	255.255.0.0	130.9.63.5	130.9.63.5	1
4	130.9.63.5	255.255.255.255	127.0.0.1	127.0.0.1	1
5	130.9.255.255	255.255.255.255	130.9.63.5	130.9.63.5	1
6	224.0.0.0	224.0.0.0	130.9.63.5	130.9.63.5	1
7	255.255.255.255	255.255.255.255	130.9.63.5	130.9.63.5	1

Ylläoleva reititystaulukko on NT-koneesta, jolla on B-luokan IP-osoite.

Taulukossa on seitsemän viitettä; rivit ovat seuraavat:

1 - reitti osoitteeseen **0.0.0.0**, on oletusreitti
2 - loopback-osoite, **127.0.0.0**
3 - verkkoreitti verkkoon **130.9.** (B-luokan osoite) - Interface-kohdassa on paikallisen verkkoliittymän osoite polkuna kyseiseen verkkoon
4 - reitti paikalliseen koneeseen (*localhost*). Huomaa, että rivillä viitataan loopback-osoitteeseen. Niin pitääkin, koska paikalliselle koneelle suunnatut tietosähkeet käsitellään sisäisesti, osoite on **130.9.63.5**
5 - aliverkon yleissanoma (*broadcast*)-osoite (interface-arvona jälleen paikallinen osoite) **130.9.255.255**
6 - multicast-osoite **224.0.0.0**
7 - rajoitettu yleissanoma (*broadcast*)-osoite, **255.255.255.255**.

Jos paketti lähetetään osoitteeseen **130.9.63.3**, taulukosta etsitään ensin reittiä kyseiseen koneeseen (jota ei löydy), sitten reittiä kyseiseen aliverkkoon (jota ei löydy), ja seuraavaksi reittiä kyseiseen verkkoon (joka löytyy). Paketti lähetetään käyttäen paikallista liittymää **130.9.63.5**. Jos paketin kohdeosoite olisi **130.10.63.5**, tehtäisiin samanlainen vertailu, mutta mitään kolmesta etsitystä reitistä ei löytyisi. Tällöin paketti lähetettäisiin oletusyhdyskäytävään, niin että kohteen MAC-osoitteeksi sijoitettaisiin oletusyhdyskäytävän MAC-osoite.

Paikallisen reititystaulukon ylläpito tapahtuu yleensä automaattisesti. Kun järjestelmä käynnistyy, viitteet paikallista verkkoa (tai verkkoja), loopback-osoitetta, multicast-osoitetta ja oletusyhdyskäytävää varten lisätään. Taulukkoon saattaa tulla enemmänkin reittejä sitä mukaa kuin IP oppii niitä. **Metric** kertoo monenko hypyn (*hop*) päässä kohde on.

Tietokone saattaa esimerkiksi vastaanottaa oletusyhdyskäytävältä viestin, jossa kerrotaan (ICMP-protokollaa käyttäen), että tiettyyn kohteeseen onkin käytettävissä aiempaa parempi reittivaihtoehto.

Oletusyhdyskäytävä

Jos oletusyhdyskäytävä ei ole käytettävissä, yhteydet paikallisen aliverkon ulkopuolelle eivät toimi. Tällaisen tilanteen varalta voidaan käyttää **useita oletusyhdyskäytäviä**. Jos käyttöön on määritetty useita oletusyhdyskäytäviä, lähetysvirheen sattuessa yritetään käyttää muita yhdyskäytäviä.

Staattinen reititys

Staattinen reititys on tilanne, jossa reitittimet eivät vaihda reititystaulujensa tietoja toistensa kanssa. Windows NT-kone voi toimia tällaisena reitittimenä kahden verkkokortin avulla. Mahdollisuudet ovat:

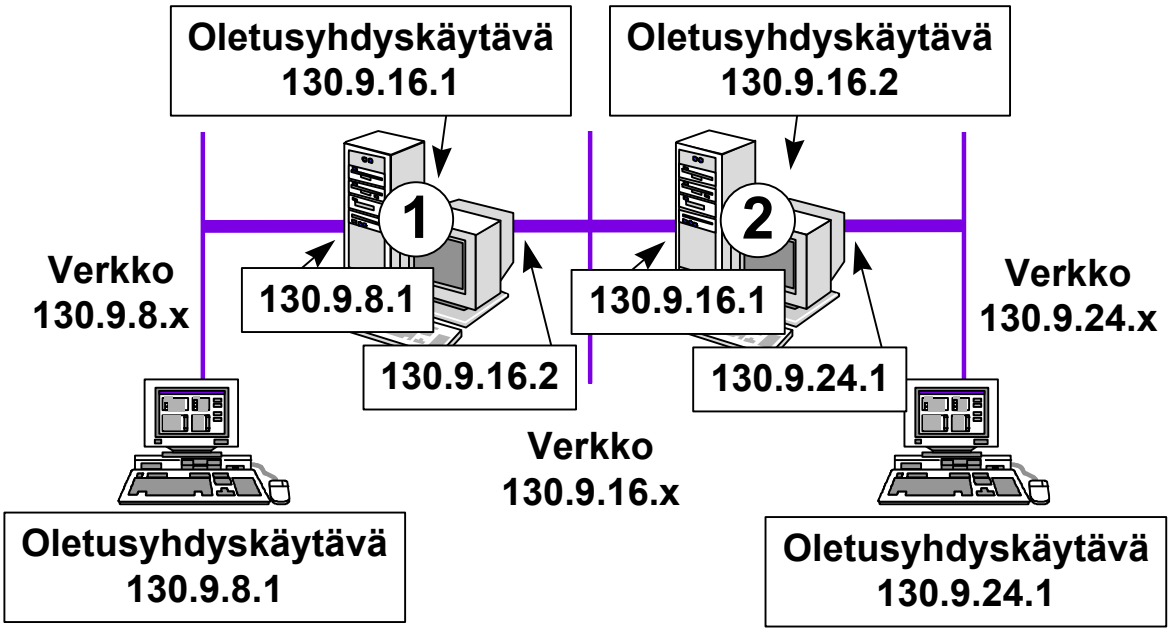
- Oletusyhdyskäytävä (**Default Gateway**)-asetukset
- **ROUTE**-komento.

Oletusyhdyskäytävä-menettelyssä voit käyttää NT-koneita, joissa on kaksi verkkokorttia, **Default Gateway**-asetusten avulla reitittimenä verkkojen välillä. Rajoituksena on toiminta vain kahden reitittimen (NT-koneen) verkoissa.

Kuvassa on havainnollistettu eri **Default Gateway**-asetukset tässä tilanteessa:

- NT-koneessa **1** on kaksi verkkokorttia (IP-osoitteet **130.9.8.1** ja **130.9.16.2**), oletusyhdyskäytävä on **130.9.16.1**

- NT-koneessa **2** on kaksi verkkokorttia (IP-osoitteet **130.9.16.1** ja **130.9.24.1**), oletusyhdyskäytävä on **130.9.16.2**.



Kun työasema verkossa **130.9.8.x** haluaa lähettää paketin verkkoon **130.9.24.x**, se tarkistaa ensin oman reititystaulunsa. Jos se ei löydä reittiä verkkoon **130.9.24.x**, se lähettää paketin oletusyhdyskäytäväänsä **130.9.8.1**. NT-kone **1** reitittää paketin edelleen kohteeseen.

Route-komento

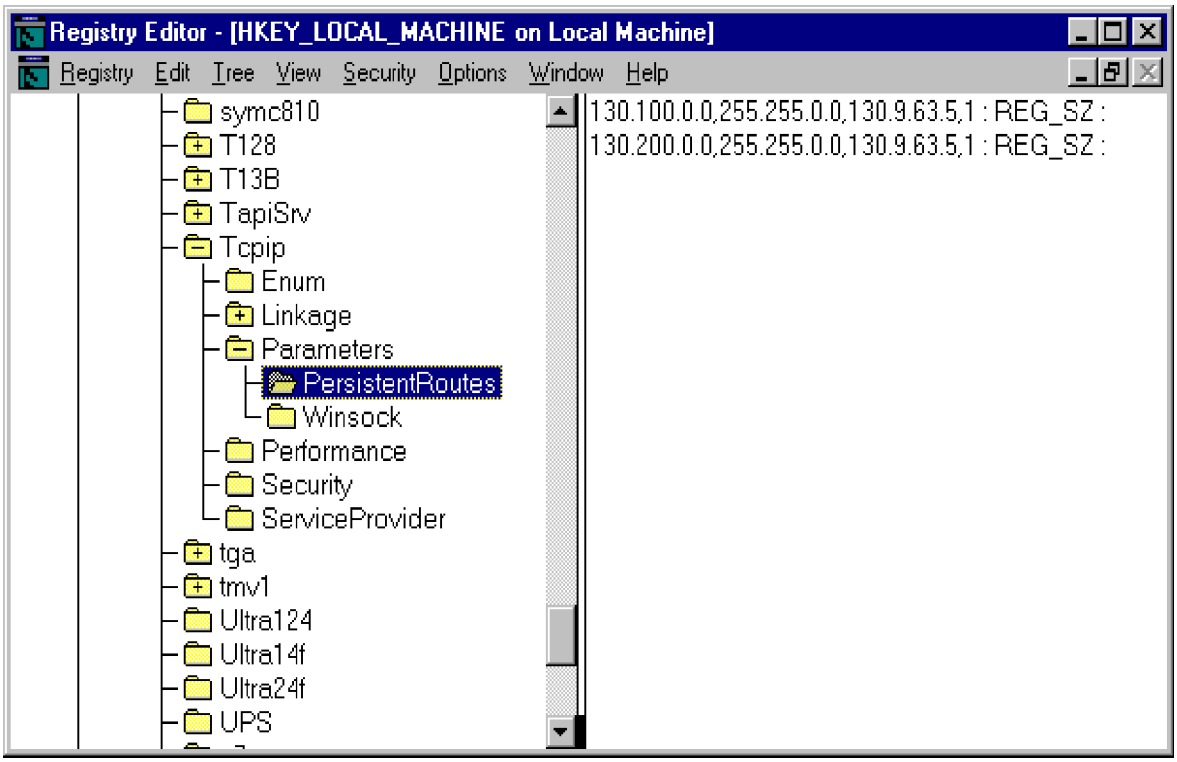
Reittejä voi lisätä myös käsin käyttämällä **route**-komentoa. Tällöin kyseessä on ns. **staattinen reititys**. Jos haluttuun kohteeseen on määritetty tällainen staattinen reititys, sitä käytetään **aina** oletusyhdyskäytävän sijasta.

Windows NT:n 3.5x- ja 4.0-versioissa komennon kanssa voi käyttää valitsinta **-p** (*persistent*), jolloin määritellystä reitistä tulee pysyvä:
route -p add 130.200.0.0 mask 255.255.0.0 130.9.63.5

Esimerkin komennossa **130.200.0.0** on kohde, **255.255.0.0** sen aliverkon maski ja **130.9.63.5** yhdyskäytävä.

Pysyvät reitit tallennetaan rekisteriin seuraavan avaimen alle:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes**



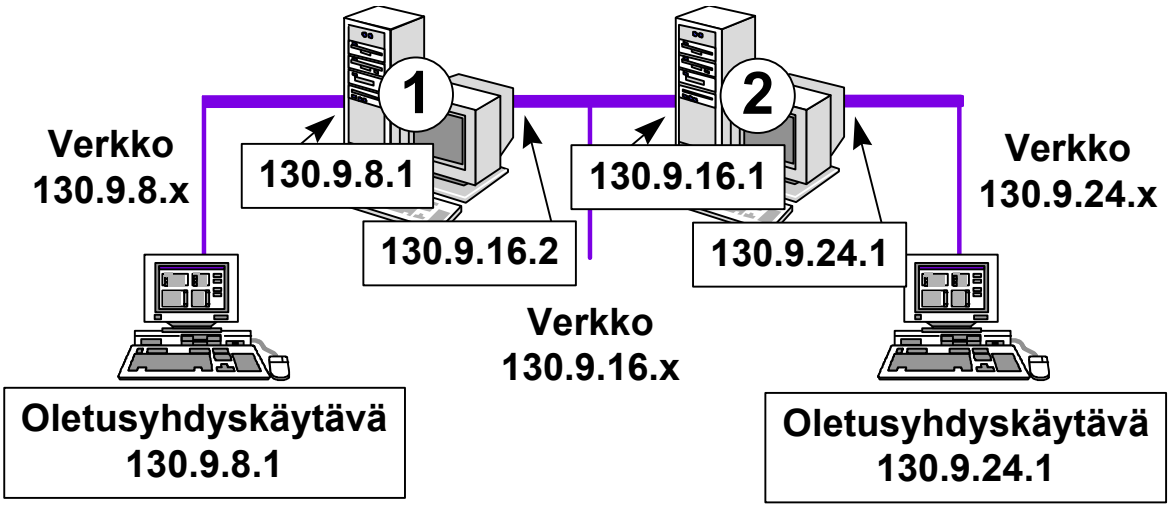
Windows NT -kone voi toimia myös verkkojen välisenä staattisena reitittimenä. Edellytyksenä ovat seuraavat toimenpiteet:

- Oikein konfiguroidut IP-osoitteet verkkokorteissa
- IP-reitityksen käyttöönotto (on asetettava käyttöön IP-protokollan **Routing**-välilehdestä)
- Määrittele staattiset reitit ROUTE-komennoilla kaikkiin verkkoihin, joihin kyseisellä NT-koneella ei ole suoraa yhteyttä.

IP-reitityksen käyttöönotto voidaan tehdä IP-protokollan **Routing**-välilehdestä ja se määritellään rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Tcpip\Parameters**
Nimi	**IpEnableRouter**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei käytössä** **1 - on käytössä**

Esimerkki reititystaulun käytöstä:



Tässä tilanteessa NT-koneiden reititystauluiksi on luotu:

NT-kone	Kohde	Yhdyskäytävä
NT-kone 1	130.9.8.0	130.9.8.1
NT-kone 1	130.9.16.0	130.9.8.2
NT-kone 1	130.9.24.0	130.9.16.1
NT-kone 2	130.9.24.0	130.9.24.1
NT-kone 2	130.9.8.0	130.9.16.2
NT-kone 2	130.9.16.0	130.9.16.1

Dynaaminen reititys

Useimmat reitittimet käyttävät jotakin protokollaa, kuten **RIP** (*Routing Information Protocol*) tai **OSPF** (*Open Shortest Path First*) vaihtaakseen reititystietoja keskenään. Tällöin kyseessä on **dynaaminen reititys**. Windows NT:n **moniprotokollareititin** tukee RIP-protokollaa.

Moniprotokollareititys

Reititysprotokollat välittävät reitittimien välillä tietoja IP-verkoista ja reitittimien välisistä linkeistä. Windows NT:n **moniprotokollareititin** on tarkoitettu pääkäyttäjille, jotka tuntevat reititysprotokollia ja -palveluita.

Windows NT:n moniprotokollareitittimen (*Multi-Protocol Router, MPR*) osat ovat:

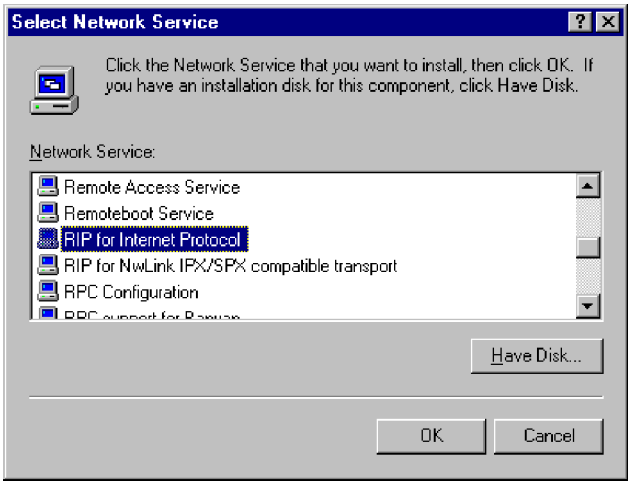
- **Routing Information Protocol (RIP) for TCP/IP** on reitittimien keskinäiseen tiedonvaihtoon käyttämä protokolla. Windows NT reitittää RIP-protokollia ja vaihtaa RIP:n avulla dynaamisesti tietoja muiden RIP:tä käyttävien reitittimien kanssa. Kaikki IP-reitittimet tukevat RIP-protokollaa

- **RIP for Internetwork Packet Exchange (IPX)** on RIP IPX (*Internetwork Packet Exchange*)-protokollalle

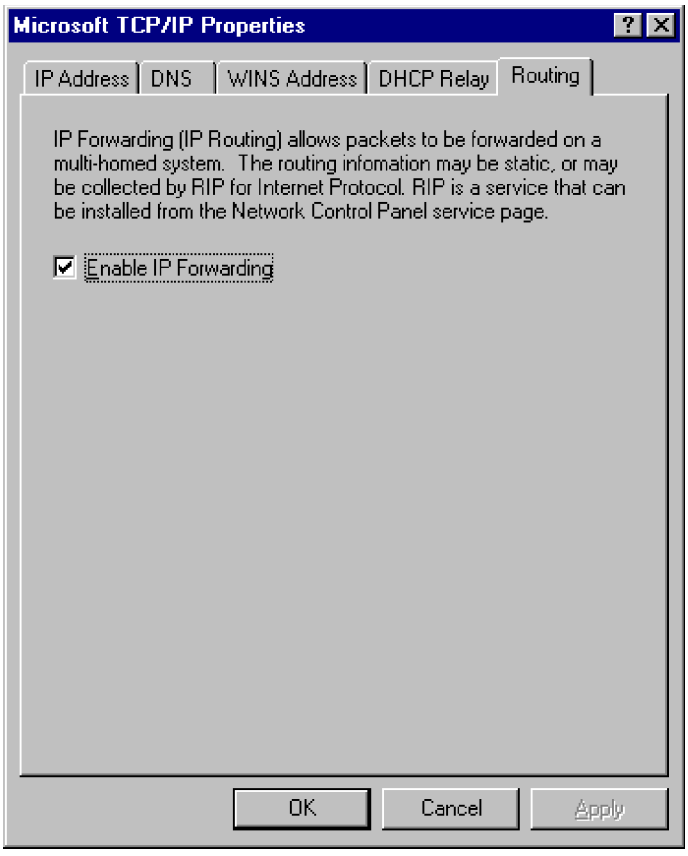
- **Boot Protocol (BOOTP) relay agent for DHCP** - Windows NT:n reititin käyttää BOOTP-agenttia välittämään DHCP-pyyntöjä DHCP-palvelimille muissa aliverkoissa. Näin yksi DHCP-palvelin voi palvella useita IP-aliverkkoja.

Routing Information Protocol (RIP) for TCP/IP

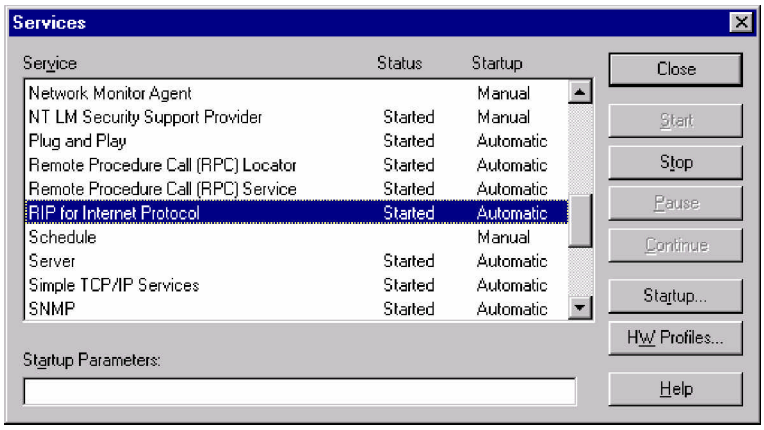
Oletusarvoisesti Windows NT -tietokoneet eivät toimi reitittiminä. Multi-Protocol Router (RIP for...) on asennettava erikseen Ohjauspaneelin **Network**-kuvakkeen **Services**-välilehdestä TCP/IP:n asentamisen jälkeen. MPR tulee Windows NT 4.0:n työasema- ja palvelinversioiden mukana.



Lisäksi on asetettava käyttöön reitityspalvelu IP-protokollan **Routing**-välilehdestä.



Tämän jälkeen reititys kahden tai useamman verkkokortin välillä käyttäen RIP-protokollaa on käytettävissä. Palvelua voi hallita Ohjauspaneelin **Services**-kuvakkeella.


Services
Service
Status
Startup
Network Monitor Agent
Manual
NT LM Security Support Provider
Started
Manual
Plug and Play
Started
Automatic
Remote Procedure Call (RPC) Locator
Started
Automatic
Remote Procedure Call (RPC) Service
Started
Automatic
RIP for Internet Protocol
Started
Automatic
Schedule
Manual
Server
Started
Automatic
Simple TCP/IP Services
Started
Automatic
SNMP
Started
Automatic
Close
Start
Stop
Pause
Continue
Startup...
HW Profiles...
Help
Startup Parameters:

Nähdäksesi reititystaulun anna komento **ROUTE PRINT**. Se kertoo NT-koneen oletuksena luoman sekä RIP:n avulla muodostaman reititystaulun. Jos NT-koneessa on vain yksi verkkokortti, RIP toimii äänettömästi (*Silent Mode*). Tällöin NT-kone vastaanottaa RIP-yleissanomat ja päivittää oman reititystaulunsa, mutta ei välitä edelleen omaan reititystauluaan.

Jos toinen verkkokortti lisätään myöhemmin, *Silent Mode* päättyy ja NT-kone alkaa automaattisesti välittää reititystietojaan. Tällöin on syytä tarkistaa, että NT-koneen asetukset ovat kunnossa, koska väärin konfiguroidut asetukset saattavat levitä vähintään koko verkon alueelle!

Jos **ROUTE PRINT** -taulukon **Metric** on suurempi kuin **1**, eikä **ROUTE ADD** -komennolla ole lisätty reititystietoja, tiedot ovat tulleet taulukkoon RIP:n kautta. **Metric** kertoo monenko hypyn (*hop*) päässä kohde on.

RAS (*Remote Access Service*) voi myös muuttaa reititystaulukon tietoja, mutta NT-kone ei kuitenkaan välitä reititystietojaan minkään muun liitännän kuin verkkokortin kautta! Siten esimerkiksi ISDN:n kautta ei välitetä reititystietoja.

Asetuksia voidaan muuttaa muokkaamalla rekisteriä suoraan (omalla vastuulla).

Tapahtumien kirjoittaminen **systeemilokiin**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\IpRip\Parameters**
Nimi	**LoggingLevel**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei merkintöjä** **1 - (oletus) vain virheet** **2 - virheet ja varoitukset** **3 - virheet, varoitukset ja tavallinen informaatio**

Silent Mode:

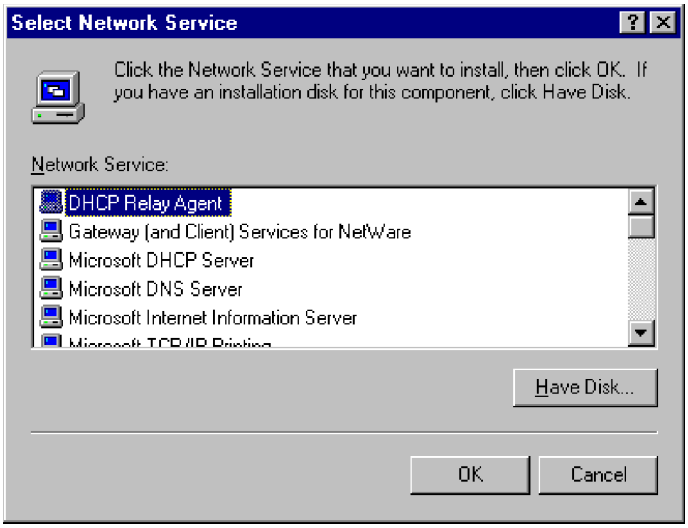
Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\IpRip\Parameters**
Nimi	**SilentRip**
Tyyppi	**REG_DWORD**
Arvo	**0 - välitä reititystietojaan automaattisesti** **1 - ei automaattisesti välitä reititystietojaan**

Koko reititystaulun päivitys:

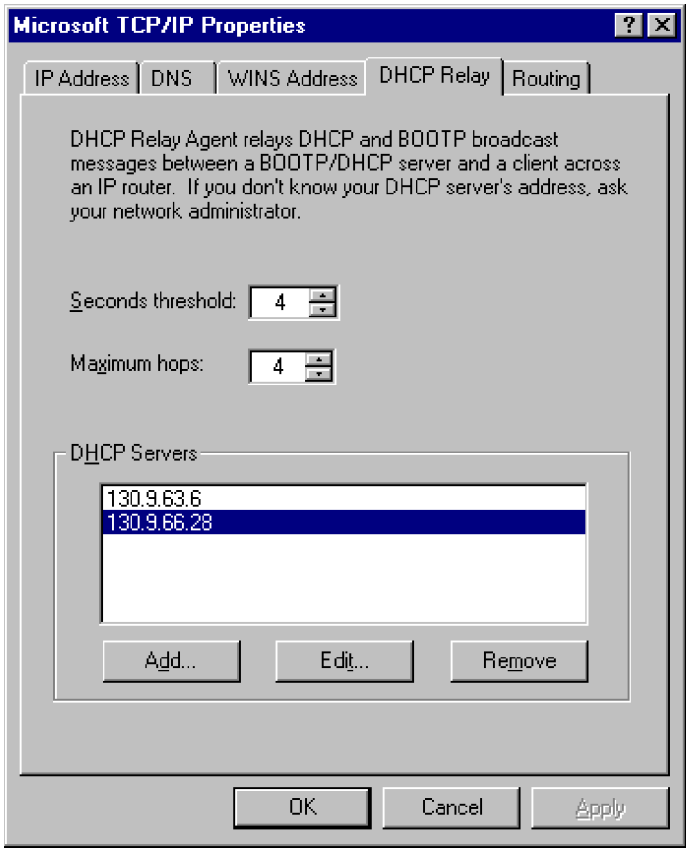
Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\IpRip\Parameters**
Nimi	**UpdateFrequency**
Tyyppi	**REG_DWORD**
Arvo	**Aika sekunteina 15 86400 (24 tuntia), oletus 30**

DHCP Relay Agent

Jos olet asentanut käyttöön Ohjauspaneelin **Network**-kuvakkeen **Services**-välilehdestä **DHCP Relay Agent** -palvelun, NT-kone voi välittää DHCP-asiakkaiden pyynnöt edelleen DHCP-palvelimelle.



Lisäksi palvelu on konfiguroitava IP-protokollan **DHCP Relay**-välilehdestä. Anna **Add**-painikkeella DHCP-palvelimien osoitteet.



Reitittäminen useiden loogisten aliverkkojen välillä

Kun samassa fyysisessä verkossa on useita loogisia aliverkkoja, käytä allaolevaa komentoa pakottaaksesi IP:n kohtelemaan kaikkia aliverkkoja paikallisina sekä käyttämään ARP:tä suoraan kohteeseen:

route add 0.0.0.0 MASK 0.0.0.0 (paikallinen_ip_osoite)

Näin paketit, jotka ovat menossa muualle kuin paikallisiin verkkoihin, lähetetään suoraan paikalliselle laitteelle eikä reitittimelle. Itse asiassa siis paikallinen verkkokortti voidaan määritellä oletusyhdyskäytäväksi. Tämä voi olla hyödyllistä, jos yhdessä fyysisessä verkossa käytetään useita C-luokan aliverkkoja ilman, että ulkomaailmaan on minkäänlaista reititinyhteyttä.

Päällekkäisten IP-osoitteiden havaitseminen

Päällekkäisten osoitteiden havaitseminen on tärkeä ominaisuus. Kun TCP/IP-pino alustetaan NT-koneen käynnistyessä, järjestelmä lähettää koko verkkoon ylimääräisen **ARP** (*Address Resolution Protocol*)-pyynnön, jossa käytetään paikallisen NT-koneen IP-osoitetta tai -osoitteita.

Mikäli tällöin jokin toinen tietokone vastaa, osoite on jo käytössä. Tällaisessakin tapauksessa NT-kone käynnistyy, mutta toisen tietokoneen kanssa päällekkäinen IP-liittymä jätetään käynnistämättä. Järjestelmälokiin jää tapauksesta merkintä ja näyttöön tulee virheilmoitus.

Jos toinen, IP-osoitteen jo varannut kone on myös NT-kone, myös sen järjestelmälokiin jää merkintä ja käyttäjälle annetaan ilmoitus. Tapahtuma ei kuitenkaan vaikuta **tämän** NT-koneen verkkotoimintoihin. Sen sijaan osoitettaan puolustava NT-kone ilmoittaa uudella ARP-viestillä verkon muille koneille, että kyseinen IP-osoite kuuluu edelleen sille. Näin muiden koneiden ARP-välimuisteissa säilyy viittaus oikeaan koneeseen.

NT-kone, jonka IP-osoite on syystä tai toisesta päällekkäinen jonkin toisen NT-koneen kanssa, voidaan aivan hyvin käynnistää silloin, kun se **ei ole kytkettynä verkkoon**. Tällöin järjestelmä ei myöskään anna mitään virheilmoitusta. Jos NT-kone myöhemmin liitetään verkkoon, virhe havaitaan.

Moniosoitteisuus

Kun samalla koneella on useampi kuin yksi IP-osoite, käytetään termiä **multihoming**. Tämä on mahdollista seuraavilla tavoilla:

- Useita osoitteita yhtä verkkokorttia kohden. **NetBT** (*NetBIOS over TCP/IP*, RFC 1001/1002) muodostaa sidoksen vain **yhteen** IP-osoitteeseen yhtä verkkosovitinta kohti. Kun NetBIOS-nimen rekisteröintiviesti lähetetään, siinä käytetään **verkkokortin IP-osoitelistan ensimmäistä osoitetta**

- Useita verkkosovittimia fyysistä verkkoa kohden - tässä ei ole muita kuin laitteistokohtaisia rajoituksia

- Useita verkkoja ja kaapelointityyppejä - ei muita kuin laitteisto- ja kaapelointikohtaiset rajoitukset.

Ohjauspaneelin kautta voidaan määritellä korkeintaan viisi IP-osoitetta samalle sovittimelle. Useampia voidaan kuitenkin lisätä muokkaamalla rekisteriä suoraan (omalla vastuulla). Oleellisia ovat seuraavat asetukset:

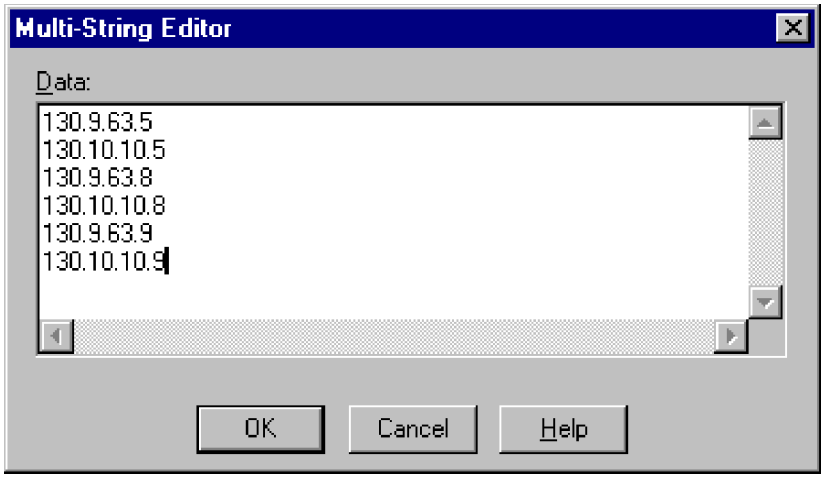
Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\(verkkokortti)\Parameters\Tcpip**
Nimi	**IPAddress**
Tyyppi	**REG_MULTI_SZ**
Arvo	**Verkkokortin ip-osoitteet**

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\(verkkokortti)\Parameters\Tcpip**
Nimi	**SubnetMask**
Tyyppi	**REG_MULTI_SZ**
Arvo	**ip-osoitteen aliverkon maski (samassa järjestyksessä kuin edellä annetut ip-osoitteet)**

Esimerkiksi:

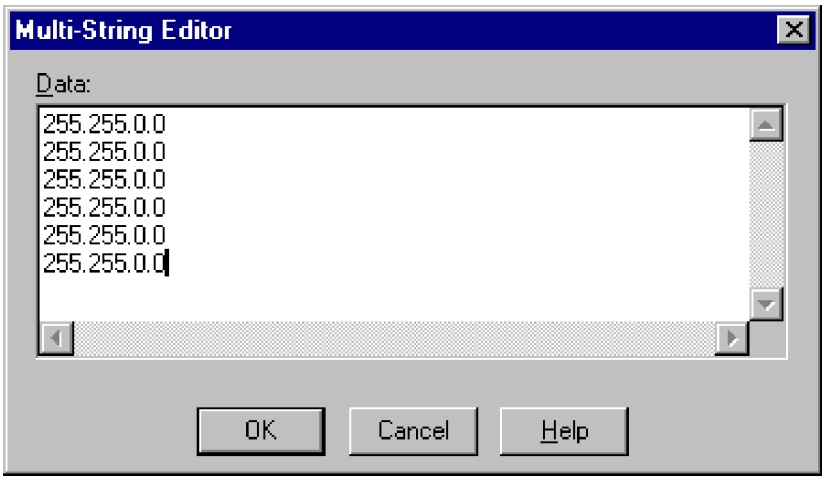
1) Käynnistä **REGEDT32.EXE** ja etsi **IPAddress**

2) Kaksoisnapauta **IPAddress**:in päälle ja anna lisättävät uudet IP-osoitteet



3) Paina **OK** ja etsi **SubnetMask**

4) Kaksoisnapauta **SubnetMask**:in päälle ja anna lisättävien uusien IP-osoitteiden aliverkkomaskit siinä järjestyksessä kuin ne liittyvät IP-osoitteisiin:



5) Paina **OK** , sulje editori ja uudelleenkäynnistä NT-kone.

Edelläolevaa esimerkkiä on kokeiltu 30 IP-osoitteella, ja se toimi.

Kun IP-tietosähke lähetetään moniosoitteisesta koneesta, se siirtyy verkkokortille, jonka reitti kohteeseen on sopivin. IP-tietosähkeeseen voi myös sisältyä lähdeosoitteena jonkin verkkokortin osoite, vaikka paketti olisikin lähtenyt jonkin toisen verkkokortin kautta. MAC-lähdeosoite sen sijaan on sen sovittimen osoite, jonka kautta paketti todellisuudessa lähti.

IP-lähdeosoite on se, minkä lähettävä sovellus määritteli ei välttämättä yksikään niistä osoitteista, joita lähettävään verkkokorttiin on Ohjaus-paneelissa liitetty.

Jos tietokoneessa on useita **verkkosovittimia**, jotka liittyvät erillisiin verkkoihin (verkkoihin, jotka eivät ole toisiinsa missään yhteydessä, esimerkiksi RAS:lla yhdistetyt verkot), saattaa tuloksena olla reitityson-gelmia. Tällöin on usein tarpeen luoda **kiinteitä** (staattisia) reittejä etäverkkoihin.

Classless Interdomain Routing

Classless Interdomain Routing (*CIDR*) tunnetaan myös nimellä **supernetting**. Sen avulla voidaan useita C-luokan verkko-osoitteita yhdistää yhdeksi loogiseksi verkoksi. CIDR määritellään RFC:ssä 1518/1519 (ftp://ds.internic.net/rfc/rfc1518.txt).

Jotta tätä menetelmää voisi käyttää, täytyy IP-osoitteiden ylempien bittien olla samat. Aliverkon peitettä puolestaan pitää lyhentää , jotta verkko-osuudesta voidaan siirtää bittejä koneosuuteen. Kun reitityspäätöksiä tehdään, vain aliverkon kattamat bitit ovat käytössä. Tällöin kaikki osoitteet näyttävät reititysmielessä kuuluvan samaan verkkoon. Kaikkien käytössä olevien reitittimien täytyy tukea CIDR:ää, ja niiden konfiguraatioihin voi joutua tekemään muutoksia.

IP Multicasting

IP Multicasting tarjoaa tehokkaat multicast-palvelut asiakkaille, jotka eivät välttämättä ole samassa verkkosegmentissä.

Nämä tietokoneet nähdään yhden IP-osoitteen kautta ja multicast-tietosähke lähetetään parhaalla mahdollisella yrityksellä (*Best Effort*) - multicast-tietosähkeen perillemenoa ei taata, ei kaikille kohteena oleville multicast-ryhmän tietokoneille eikä myöskään taata pakettien saapumista perille oikeassa järjestyksessä. Multicast-ryhmään voi liittyä ja poistua dynaamisesti.

Windows Sockets -ohjelmat voivat liittyä multicast-ryhmään.

Windows NT:n versiot 3.5x ja 4.0 ovat yhteensopivia RFC 1112 -määrityksen tason 2 kanssa (sisältää sekä lähetyksen että vastaanoton). IP multicastingissa käytettävät protokolla on **Internet Group Management Protocol** (IGMP).

Käytännön sovelluksena IP-multicastingille nähdään mm. tilausperusteiset jakelut; uutiset, videostreamit jne.

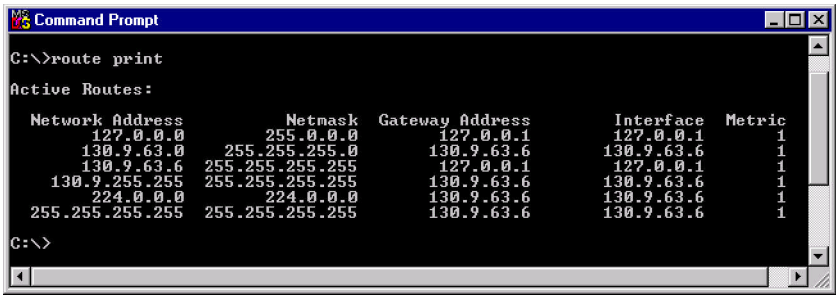
Internet Control Message Protocol

Internet Control Message Protocol (ICMP) on ylläpitoprotokolla, joka kuvataan RFC 792:ssa. Sen katsotaan yleensä kuuluvan IP-kerrokseen. ICMP-viestit on kapseloitu IP-datagrammeihin, joten niitä voidaan reitittää läpi verkon. Windows NT käyttää ICMP:tä seuraaviin tarkoituksiin:

- Reititystaulujen rakentaminen ja ylläpito
- **Path Maximum Transfer Unit** (PMTU) -havainnot
- Ongelmanratkaisu ja diagnostiikka (ping- ja tracert-työkaluilla)
- Vuonohjauksen säätelyyn, jotta estetään linkin tai reitittimen ylikuormitus.

Reititystaulujen ylläpito

Kun Windows NT -kone käynnistyy, reititystaulukko koostuu tavallisesti vain muutamasta rivistä. Yksi noista riveistä on oletusyhdyskäytävä. Paketit, joiden kohdeosoitteelle ei löydy muuta reittiä, lähetetään oletusyhdyskäytävälle.



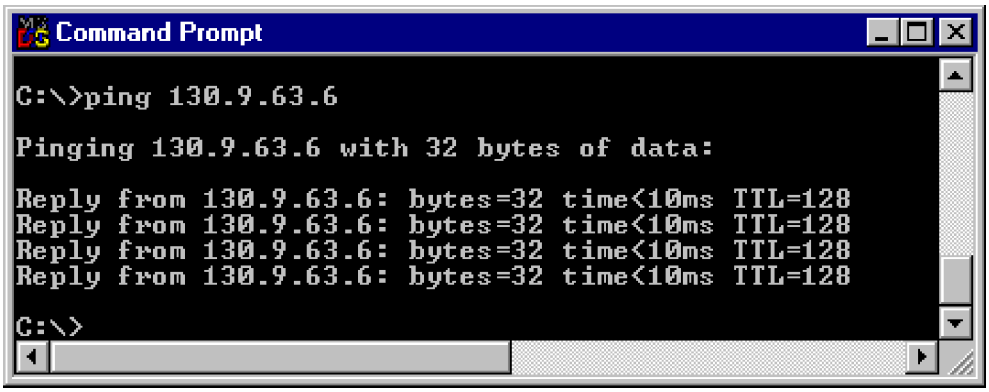
Koska reitittimet kuitenkin vaihtavat keskenään tietoa verkon topologiasta, oletusyhdyskäytävä saattaa tuntea paremman reitin haluttuun päämäärään. Kun näin käy, oletusyhdyskäytävä lähettää paketin edelleen aivan normaalisti, mutta kertoo sitten alkuperäiselle lähettäjälle ICMP:n uudelleenohjausviestillä, että parempikin reitti on olemassa.

Näiden viestien avulla voidaan määritellä uudelleenohjaus yhdelle koneelle, aliverkolle tai kokonaiselle verkolle. Kun NT-kone vastaanottaa ICMP:n uudelleenohjausviestin, se tarkistaa, tuliko viesti ensimmäiseltä reitin varrella olevalta yhdyskäytävältä ja onko kyseinen yhdyskäytävä suoran verkkoyhteyden päässä. Jos näin on, Windows NT muokkaa reititystaulukkoa lisäämällä kohteeseen paremman reitin.

Jos uudelleenohjausviesti ei tullut lähimmältä yhdyskäytävältä tai jos kyseinen laite ei ole suoran verkkoyhteyden päässä, muutoksia ei tehdä. TCP käyttää **Path Maximum Transfer Unit** -havaitsemista. Järjestelmä on riippuvainen ICMP:n viesteistä, jotka viittaavat kohteen saavuttamattomuuteen (*destination unreachable*).

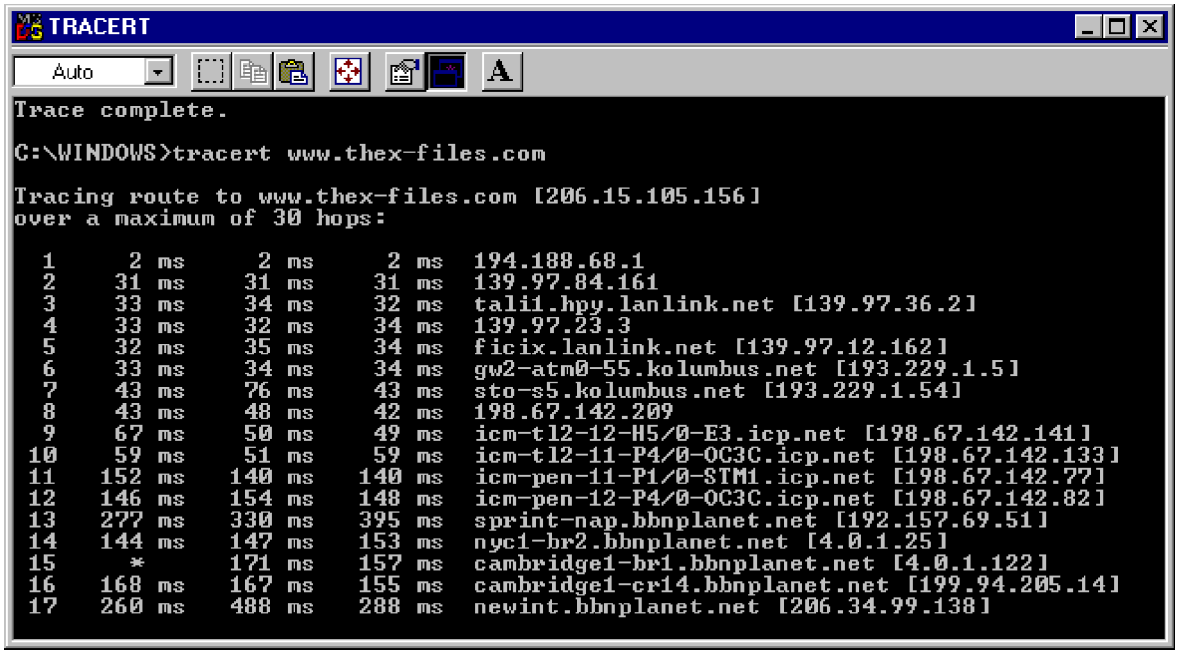
Ongelmanratkaisu ICMP:n avulla

Ping-apuohjelma lähettää ICMP:n kaiutuspyyntöjä tiettyyn IP-osoitteeseen ja odottaa ICMP-vastauksia. **Ping** raportoi saamansa vastaukset sekä niiden saapumiseen kuluneet ajat. Komennolle on monia komentorivivalitsimia, joista esimerkissä käytetään kohteen osoitetta.



Tracert on reitinseurantatyökalu, joka voi osoittautua hyvin hyödylliseksi. Se lähettää ICMP:n **echo**-pyyntöjä tiettyyn IP-osoitteeseen ja kasvattaa IP-otsikossa olevaa **time-to-live**-arvoa (TTL) aina yhdellä (alkuarvona on 1) sekä analysoi vastauksena tulleet viestit ja virheet. Jokaisen onnistuneen pyynnön pitäisi päästä hyppäyksen verran eteenpäin kohti seuraavaa reititintä, ennen kuin TTL saa arvon nolla ja vastauksena pakettia kuljettavalta reitittimeltä tulee ICMP:n **time exceeded** -viesti.

Tracert tulostaa jokaisen reitin varrella olevan reitittimen tiedot järjestyksessä lähimmästä kaukaisimpaan. Jos komentorivillä käytetään valitsinta **-d**, reitittimien IP-osoitteita vastaavia DNS-nimiä ei selvitetä. Tällöin listassa näkyy vain kunkin reitittimen IP-osoite.



Vuonohjauksen säätely ICMP:n avulla

Jos jokin tietokone lähettää tietosähkeitä toiselle tietokoneelle liian innokkaasti, reitin varrella olevat reitittimet ja linkit saattavat mennä tukkoon. Tällöin lähettävä kone saattaa saada ICMP:n **lähteen hiljennys** (*source quench*) -viestin, joka kehottaa sitä hidastamaan vauhtia.

Windows NT:n TCP/IP reagoi tähän viestiin, mikäli se sisältää otsikkotietoja jostakin kyseisen NT-koneen aktiivisen TCP-yhteyden yli lähettämästä tietosähkeestä.

Jos Windows NT -konetta käytetään reitittimenä ja sen pakettien vastaanottopuskuri täyttyy, osa paketeista putoaa pois. NT-reititin ei kuitenkaan lähetä **lähteen hiljennys** -viestejä pakettien alkuperäisille lähettäjille.

Internet Group Management Protocol

IP-multicasting tarkoittaa IP-tietosähkeen lähettämistä vastaanottajaryhmälle yhden vastaanottajan sijasta. Ryhmään voi kuulua nolla tai useampia koneita, ja koko koneryhmää vastaa yksi IP-osoite. Tietosähke toimitetaan kaikille vastaanottajille samojen periaatteiden mukaan kuin lähetettäessä yhdelle vastaanottajalle, eli kaikkien pakettien ei voida taata saapuvan perille, eivätkä paketit välttämättä saavu kaikille vastaanottajille samassa järjestyksessä suhteessa muihin paketteihin.

Vastaanottajaryhmä on dynaaminen, toisin sanoen tietokone voi liittyä siihen tai erota siitä tarpeen mukaan. Ryhmän jäsenten sijainnille tai määrälle ei ole rajoituksia. Tietokone voi kuulua samaan aikaan useampaankin ryhmään, mutta sen ei tarvitse kuulua tiettyyn ryhmään kyetäkseen lähettämään kyseiselle ryhmälle paketteja.

Ryhmä voi olla pysyvä tai väliaikainen. Pysyvällä ryhmällä on tunnettu, ylläpitäjien antama IP-osoite. Osoite on pysyvä, eivät ryhmän jäsenet: ryhmän jäsenmäärä saattaa vaihdella ja olla jopa nolla. Sellaisia IP-osoitteita, joita ei ole varattu pysyvien ryhmien käyttöön, voidaan käyttää tilapäisille ryhmille. Tällainen osoite vapautuu aina, kun ryhmän jäsenmäärä laskee nollaan.

Multicast-tietosähkeen edelleenlähettämisen hoitavat multicast-reitittimet. Ne saattavat toimia yhdessä yhdyskäytävien kanssa tai erillisinä laitteina. Kukin tietokone lähettää multicast-tietosähkeen paikalliseen verkkoon, jolloin se tavoittaa kaikki lähinnä olevat vastaanottajaryhmän koneet. Jos IP-tietosähkeen **time-to-live-arvo** on suurempi kuin yksi, verkkoon liitetty multicast-reititin välittää sen eteenpäin kaikille niille verkoille, joissa on vastaanottajaryhmän jäseniä. Jos tällaisen verkon tavoittaminen onnistuu **time-to-live-ajan** kuluessa, vastaanottava reititin hoitaa tietosähkeen jakelun vastaanottajille jälleen paikallisena multicast-lähetyksenä.

Windows NT:n versiot 3.5x ja 4.0 sisältävät RFC 1112:n mukaiset IP multicasting -ominaisuudet.

Tällä hetkellä ainoastaan **Windows Internet Name Service** (WINS) käyttää IGMP-protokollaa etsiessään replikointipalvelimia multicast-menetelmällä.

IP/ARP-laajennukset ja multicasting

Jotta IP-multicasting onnistuisi, on määriteltävä ylimääräinen reitti. Tämä reitti (joka lisätään oletusarvoisesti) pakottaa lähettämään multicast-tietosähkeet paikallisen verkkokortin kautta, ei oletusyhdyskäytävän. Seuraava reitti (jonka voi tulostaa komennolla **route print**) kuvaa tilannetta:

Network Address	Netmask	Gateway Address	Interface	Metric
224.0.0.0	224.0.0.0	130.9.63.1	130.9.63.5	1

Ryhmäosoitteet on helppo tunnistaa, koska ne ovat aina **D-luokan** osoitteita välillä **224.0.0.0-239.255.255.255**. Kaikkien näiden osoitteiden neljä ylintä bittiä ovat **1110**.

Jotta paketin lähettäminen vastaanottajaryhmälle paikallisen verkkokortin kautta onnistuisi, IP-osoite täytyy muuntaa MAC-osoitteeksi. IP-ryhmäosoite muunnetaan Ethernetin multicast-osoitteeksi asettamalla Ethernet-osoitteen 23 alinta bittiä samoiksi kuin IP-osoitteen 23 alinta bittiä. Koska jokaisessa IP-osoitteessa on 28 merkitsevää bittiä, useampi kuin yksi vastaanottajaryhmä voi käyttää samaa Ethernet-osoitetta. Koska useampi kuin yksi IP-multicast-osoite saattaa muuntua samaksi Ethernet-multicast-osoitteeksi, verkkosovitin saattaa ilmoittaa multicasteista ryhmälle, jota yksikään paikallinen sovellus ei ole ilmoittanut käsittelevänsä. Tällaiset ylimääräiset multicastit hylätään. Protokollapinon täytyy lisäksi tarjota vielä keinot ryhmään liittymiseen ja siitä poistumiseen.

IP-multicasting ja Windows Sockets -ohjelmat

Oletusarvoisesti multicast-tietosähkeet lähetetään **time-to-live**-arvolla (TTL) **1** ja sovellus voi käyttää **setsockopt()-kutsua** TTL-arvon asettamiseen. Multicast-reitittimet käyttävät TTL-arvoa päätelläkseen, kuinka pitkälle tietosähke pitää lähettää edelleen.

TTL-raja-arvot Windows Sockets -sovelluksille:

TTL-raja-arvo	Kuvaus
TTL=0	Rajoitettu samaan koneeseen (*host*)
TTL=1	Rajoitettu samaan aliverkkoon (*subnet*)
TTL=32	Rajoitettu samaan palvelinalueeseen (*site*)
TTL=64	Rajoitettu samalle alueelle (*region*)
TTL=128	Rajoitettu samalle mantereelle (*continent*)
TTL=255	Ei rajoitettu

Transmission Control Protocol

Transmission Control Protocol (TCP) tarjoaa yhteyspohjaisen, luotettavan kuljetuspalvelun ohjelmille. Microsoft-verkko käyttää TCP:tä kirjautumiseen, tiedostojen ja kirjoitinten jakamiseen, informaation monistamiseen ohjauskoneiden (*domain controller*) välillä, selauspalvelun (*Browser*) listojen siirtoon ja moniin muihin tarkoituksiin. TCP:tä voi kuitenkin käyttää vain kahdenväliseen viestintään. TCP valvoo **tarkistussumman** avulla, että otsikko- ja datatiedot eivät vääristy paketin kulkiessa verkossa.

TCP:n vastaanottoikkunan koko

TCP:n **vastaanottoikkunan** (*Receive window*) koko tarkoittaa sitä datamäärää (tavuina), joka kerrallaan voi olla yhteyspuskurissa. Lähettävä tietokone pystyy lähettämään ainoastaan vastaanottoikkunan verran tavuja, ennen kuin jää odottamaan **kuittausta** (ACK) ja ikkunan päivitystä.

TCP/IP-pino on suunniteltu niin, että se hienosäätää itse itseään useim-

missa ympäristöissä. Sen sijaan, että vastaanottoikkunan koko olisi kiinteä, TCP säätää sen kokoa. Segmentin **maksimikoko** (*Maximum Segment Size*, MSS) neuvotellaan aina yhteyden aluksi, ja TCP voi lisätä vastaanottoikkunan kokoa MSS:n monikertoina.

MSS:n monikertojen käyttäminen ikkunan koon kasvattamiseen lisää kokonaisten TCP-segmenttien osuutta koko datasta tiedonsiirron aikana.

Vastaanottoikkunan oletusarvot ovat:

TCPWindowSize = 8 kt pyöristettynä ylöspäin lähimpään MSS:n monikertaan; jos tämä ei ole vähintään **4 * MSS**, kokoa lisätään niin että se on **4 * MSS**, kuitenkin enintään **64 kt**. Tämä on vastaanottoikkunan suurin koko, koska TCP-otsikko on 16-bittinen. RFC 1323 määrittelee keinon suurentaa TCP-ikkunan kokoa, mutta Windows NT:n TCP/IP ei vielä tue sitä.

Ethernetissä ikkunan koko on normaalisti **8760** tavua (8192 pyöristettynä ylöspäin, niin että lopputuloksena on **6 * 1460** tavun kokoinen puskuri). FDDI- tai Token Ring -verkossa arvo on noin 16 kt. Nämä ovat oletusarvoja, eikä niitä yleensä ole syytä muuttaa. Jos haluat muuttaa oletusarvoa, muokkaa järjestelmärekisterin parametria **TcpWindowSize** muuttaaksesi arvoa pysyvästi tai käytä sovelluksessa **setsockopt()**-kutsua muuttaaksesi arvoa yhteyskohtaisesti. Asetus löytyy rekisteristä TCP/IP:n parametrien kohdalta.

Viivästetyt kuittaukset

TCP käyttää viivästettyjä kuittauksia (*delayed acknowledgment*) vähentääkseen verkossa liikkuvien pakettien määrää (RFC 1122). Kuittaus lähetetään, jos seuraavat ehdot täyttyvät:

- ACK-viestiä ei ole lähetetty edellisen saapuneen segmentin jälkeen
- Viimeksi saapuneen segmentin jälkeen ei ole saapunut uutta segmenttiä 200 millisekuntiin.

Toisin sanoen, normaalisti kuittaus lähetetään joka toisen segmentin jälkeen, ellei segmenttien väli kasva 200 millisekuntiin. Viivästettyjä kuittauksia ei voi kytkeä pois käytöstä millään rekisteriasetuksella.

PMTU-havaitseminen

RFC 1191:ssä määritellään **PMTU-havaitseminen**. Kun yhteys muodostetaan, tietokoneet vaihtavat TCP:n MSS (*Maximum Segment Size*)-arvojaan. Pienempi kahdesta MSS-arvosta otetaan käyttöön yhteyden ajaksi. Yleensä tietokoneen MSS-arvo on MTU (Maximum Transfer Unit) vähennettynä IP- ja TCP-otsikoiden vaatimilla 40 tavulla.

Kun TCP-segmenttien määränpää on paikallisen verkon ulkopuolella, IP-otsikon älä fragmentoi -bitti asetetaan. Matkan varrella olevien reitittinten ja verkkojen MTU-arvo saattaa olla erisuuruinen kuin lähettävän ja vastaanottavan tietokoneen MTU. Jos reitin varrella oleva reititin havaitsee, että verkon MTU on pienempi kuin lähetettävä tietosähke, se yrittää fragmentoida tietosähkeen pienemmiksi paloiksi. Tätä yrittäessään reititin kuitenkin huomaa, että fragmentoinnin estävä bitti on päällä. Tällöin reitittimen pitäisi lähettää takaisin ICMP **destination unreachable** -viesti, joka kertoo, että tietosähkettä ei voi lähettää edelleen ilman pilkkomista pienempiin osiin. Useimmat reitittimet palauttavat samalla myös reitin seuraavan välin suurimman mahdollisen MTU-arvon; arvo sijoitetaan 16 alimpaan bittiin siihen ICMP-otsikon kenttään, joka ICMP-määrityksen mukaan on käyttämätön .

Kun alkuperäinen lähettäjä saa tämän viestin, TCP muuttaa MTU-arvoa niin, ettei se ole suurempi kuin suurin sallittu arvo. MTU:hun tulee mahtua lisäksi TCP- ja IP-otsikot. Pienin sallittu MTU on 68 tavua, ja Windows NT noudattaa tätä raja-arvoa.

Jotkin epästandardit reitittimet saattavat kaikessa hiljaisuudessa pudottaa liian suuria IP-paketteja ilman, että kertovat siitä lähettäjälle. Jotkin reitittimet saattavat myös raportoida virheellisen MTU-arvon.

Tällaisista käytetään nimitystä **Musta aukko** (*Black Hole*) -reitittimet.

Jos näin käy, saattaa olla tarpeen muuttaa PMTU:n havaitsemisalgoritmia. PMTU-muutokset voidaan tehdä muuttamalla kahta rekisteriparametria:

- **EnablePMTUBHDetect** muuntaa algoritmia niin, että ongelmalliset musta aukko -reitittimet (BH, *black hole*) löytyvät. Tällä menetelmällä havaitaan toistuvat ACK:it ja fragmentoitumisen estobitti poistetaan. Ominaisuus ei ole käytössä oletusarvoisesti. Voit poistaa asetuksen käytöstä poistamalla nimen tai anta-

malla arvoksi **0**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Parameters\Tcpip**
Nimi	**EnablePMTUBHDetect**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei käytössä** **1 - käytössä**

- **EnablePMTUDiscovery**-arvon muuttaminen joko ottaa käyttöön tai poistaa käytöstä koko PMTU-havaitsemisen. Jos toiminto ei ole käytössä, MTU:n arvona on 576 tavua kaikille eipaikallisille osoitteille. Tämä toiminto on oletusarvoisesti käytössä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\Parameters\Tcpip**
Nimi	**EnablePMTUDiscovery**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei käytössä** **1 - käytössä**

Kahden tietokoneen välinen PMTU voidaan testata **Ping**-ohjelmalla käyttämällä valitsinta **-f** (ei fragmentointia) seuraavasti:

ping -f -n (pingien määrä) -l koko (ip-osoite)

Tämän esimerkin koko-parametria voidaan kasvattaa, kunnes MTU löytyy. Huomaa, että **Pingin** käyttämä koko on lähetettävän datapuskurin koko eikä sisällä otsikkoja. ICMP-otsikko vie 8 tavua ja IP-otsikko tavallisesti 20 tavua.

Seuraavassa tapauksessa (Ethernet) linkkikerroksen MTU on maksimikokoinen **ping**-puskuri plus 28, eli 1500 tavua:

```
C:\WINNT>ping ftp.eunet.fi
Pinging gromit.eunet.fi [193.66.1.49] with 32 bytes of data:
Reply from 193.66.1.49: bytes=32 time=31ms TTL=248
Reply from 193.66.1.49: bytes=32 time=29ms TTL=248
Reply from 193.66.1.49: bytes=32 time=29ms TTL=248
Reply from 193.66.1.49: bytes=32 time=31ms TTL=248

C:\WINNT>ping -f -n 1 -l 1472 193.66.1.49
Pinging 193.66.1.49 with 1472 bytes of data:
Reply from 193.66.1.49: bytes=1472 time=426ms TTL=248

C:\WINNT>ping -f -n 1 -l 1473 193.66.1.49
Pinging 193.66.1.49 with 1473 bytes of data:
Packet needs to be fragmented but DF set.
```

Edellisessä esimerkissä reititin palautti ICMP-virheilmoituksen, jonka ping tulkitsi. Jos kyseessä olisi ollut musta aukko -tyyppinen reititin, ping ei yksinkertaisesti olisi saanut vastausta, koska MTU olisi ollut reitittimelle liian suuri. Näin Ping-ohjelmaa voidaan käyttää mustien aukkojen etsimiseen verkosta.

Kuolleen yhdyskäytävän havaitseminen

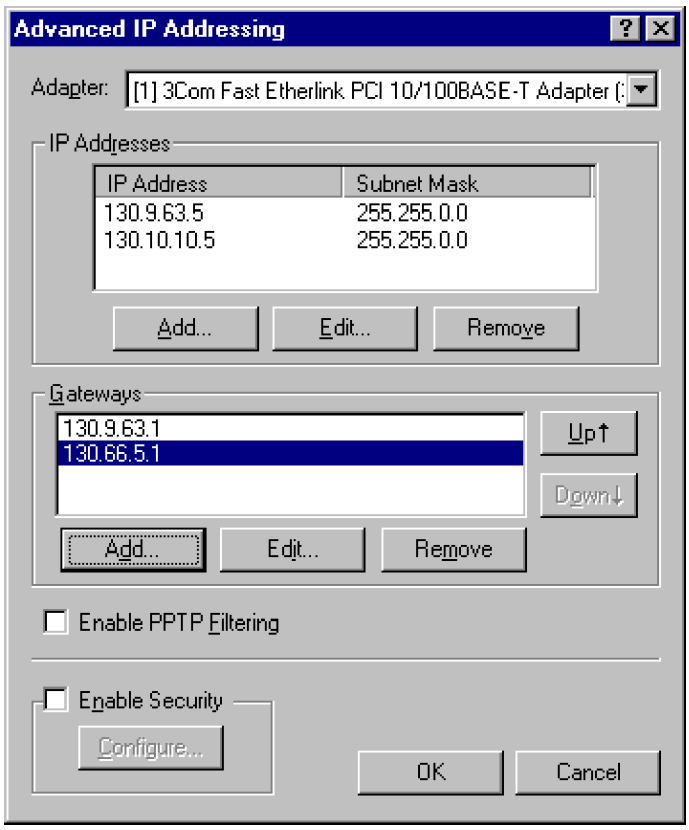
Microsoft TCP/IP:n ominaisuuksiin kuuluu kuolleen yhdyskäytävän (*Dead Gateway*) havaitseminen. Tämän ominaisuuden avulla TCP pystyy tunnistamaan viat oletusyhdyskäytävän toiminnassa ja muokkaamaan IP-reititystaulukkoa niin, että reititykseen käytetään jotakin toista yhdyskäytävää.

Kuolleiden yhdyskäytävien havaitsemiseen käytetään TCP-uudelleenlähetystä. Microsoftin TCP/IP käyttää *triggered reselection* -keinoa (kuvattu RFC 816:ssä).

TCP yrittää lähettää oletusyhdyskäytävälle pakettia, kunnes saa kuittauksen tai kunnes puolet rekisteriparametrin **TcpMaxDataRetransmissions** arvosta täyttyy. Oletusarvo on **5**.

Jos oletusyhdyskäytävä ei vastaa ja useampia kuin yksi yhdyskäytävä on konfiguroitu, TCP pyytää IP:tä siirtymään seuraavan listalla olevan yhdyskäytävän käyttäjäksi.

Voit lisätä yhdyskäytäviä **Gateways**-kohtaan **Advanced IP Addressing** -ikkunassa (katso myös tarvittaessa kirjan lukua **3**).



Jos NT-kone on DHCP-asiakas, oletusyhdyskäytävä konfiguroidaan automaattisesti.

Pingin kaltaiset työkalut eivät laukaise kuolleen yhdyskäytävän havaitsemisprosessia, vaan käyttävät oletusyhdyskäytävää. Jos TCP havaitsee kuolleen yhdyskäytävän ja valitsee uuden, IP-työkalut alkavat käyttää uutta yhdyskäytävää. Kuolleen yhdyskäytävän havaitsemistoiminto on oletusarvoisesti käytössä, jos NT-koneelle on määritelty useampi kuin yksi yhdyskäytävä.

Uudelleenlähetys

TCP käynnistää uudelleenlähetysajastimen aina, kun lähetettävä segmentti siirretään IP:lle. Jos kuittausta ei kuulu määräajan kuluessa, segmentti lähetetään uudelleen korkeintaan niin monta kertaa kuin asetuksen **TcpMaxDataRetransmissions** arvona on. Oletusarvo on **5**. Jos rekisteriparametrin arvoa lisätään yhdellä, kaikkien yhteyksien aikakatkaisuarvot suurinpiirtein kaksinkertaistuvat.

Uudelleenlähetyksen ajastin alustetaan kolmeen sekuntiin, kun TCP-yhteys muodostetaan. TCP kuitenkin muuttaa arvoa yhteyden aikana sen mukaan, kuinka hyvä tai huono yhteys on. Tähän käytetään *smoothed round trip time* -laskelmaa (SRTT) RFC:n 793 mukaisesti. Kunkin segmentin ajastimen arvo tuplataan jokaisella uudelleenlähetyskerralla. Tätä algoritmia käyttämällä TCP säätää toimintaansa aina normaalin yhteysviiveen mukaiseksi. Jos TCP-yhteyden viiveet ovat keskimäärin suuria, järjestelmä odottaa ennen uudelleenlähetystä pitempään kuin silloin, jos yhteysviiveet saman yhteyden aikana ovat olleet hyvin pieniä. Jos esimerkiksi NT-työasema on yhteydessä ftp:llä samassa Ethernet-segmentissä ja aliverkossa olevaan NT-palvelimeen, niin yhteys on todennäköisesti hyvä ja SRTT-arvo näin ollen pieni. Jos kesken yhteyden toinen NT-koneista irrotetaan verkosta, ensimmäinen uudelleenlähetys tapahtuu jo noin puolen sekunnin kuluttua virheestä. Sen jälkeen ajastimen arvo tuplataan jokaisella uudelleenlähetyskerralla. Viidennen uudelleenlähetyskerran (TcpMaxDataRetransmissions-arvo) jälkeen ajastinta kasvatetaan jälleen kaksinkertaiseksi, ja jos kuittausta ei vieläkään kuulu, yhteys katkaistaan.

TCP:n keepalive-viestit

TCP-yhteyden auki pitämiseksi tarkoitettu keepalive-paketti on ACK-viesti, jonka sarjanumero on yhtä pienempi kuin senhetkinen viimeisin sarjanumero. Tietokoneen, joka vastaanottaa tällaisen viestin, tulisi vastata ACK-viestillä, jonka sarjanumero on sama kuin senhetkinen viimeisin sarjanumero (siis yhtä isompi kuin keepalive-viestissä).

Näillä viesteillä voidaan varmistaa, että toisessa päässä oleva laite on vielä käytettävissä. Keepalive-viestejä lähetetään tasaisin väliajoin, ja väliaika määritellään rekisteriparametrilla **KeepAliveTime**. Oletusarvo on 7 200 000 millisekuntia eli kaksi tuntia.

Niitä lähetetään vain silloin, jos muuta dataa tai korkeamman tason keepalive-viestejä ei ole lähetetty tai vastaanotettu kyseisenä aikana. Jos keepalive-viestiin ei saavu vastausta, viestiä lähetetään uudelleen parametrissa **KeepAliveInterval** määrätyin välein. Oletusarvo on yksi sekunti.

NetBT (*NetBIOS Over TCP/IP*)-yhteydet, joita monet Microsoftin verkkokomponentit käyttävät, lähettävät NetBIOS-keepalive-viestejään tavallisesti paljon tiheämmin, joten TCP:n ei yleensä tarvitse lähettää vastaavia viestejä NetBIOS-yhteyden yli.

TCP:n keepalive-toiminto ei ole oletusarvoisesti käytössä, mutta **Windows Sockets** -ohjelmat voivat ottaa sen käyttöön **setsockopt()**-kutsulla.

Ylikuormituksen välttäminen

Kun yhteys muodostetaan, TCP käyttää hidasta nopeutta yhteyden suorituskyvyn arviointiin. Tällöin vastaanottajalaitteella tai yhteyden varrella olevilla laitteilla ei ole vaaraa ylikuormituksesta. Lähetysikkunan koko on aluksi kaksi TCP-segmenttiä.

Jos TCP/IP-segmentit kuitataan, lähetysikkunaa suurennetaan niin kauan, kunnes se saavuttaa saman koon kuin vastaanottavan järjestelmän vastaanottoikkuna. Tästä eteenpäin hidasta aloitusalgoritmia ei enää käytetä, ja vuonohjauksen hoidetaan etäkoneen vastaanottoikkunan mukaan.

Jos kuitenkin missä tahansa vaiheessa yhteyden aikana ilmenee ylikuormitusta (josta on merkkinä uudelleenlähetysten tarve), käytetään ylikuormitusta ehkäisevää algoritmia pienentämään lähetysikkunaa tilapäisesti. Ikkunan koko kasvatetaan hiljalleen takaisin entiselleen ylikuormituksen hävittyä.

Näistä algoritmeista löydät lisää tietoa RFC:stä 1122.

Silly Window Syndrome

RFC 1122 kuvaa ilmiötä nimeltä **Silly Window Syndrome** (SWS). SWS:n aiheuttaa se, että vastaanottaja kasvattaa vastaanottoikkunaa aina, kun uutta puskuritilaa tulee käyttöön ja vastaavasti lähettäjä käyttää enemmän ikkunatilaa lähettääkseen enemmän dataa. Tuloksena voi olla, että tietokoneiden välillä siirretään pieniä segmenttejä, vaikka kokonaisuudessaan puskuritilaa olisikin paljon.

Windows NT:n TCP/IP ehkäisee SWS:ää RFC 1122:n mukaisesti eikä lähetä enempää dataa, ennen kuin vastaanottaja kertoo käytettävissä olevan riittävästi ikkunatilaa kokonaisten segmenttien siirtämiseen. Vastaanottaessaan dataa NT ehkäisee SWS:ää vastaavalla tavalla: se ei suurenna vastaanottoikkunaa, ellei puskuritilaa ole riittävästi kokonaisen segmentin vastaanottoon.

Nagle-algoritmi

Windows NT:n TCP/IP käyttää RFC 896:n mukaista Nagle-algoritmia. Tämän algoritmin tarkoitus on vähentää pienten segmenttien lähettämistä erityisesti yhteyksillä, joissa viive on suuri. Nagle-algoritmi sallii kerrallaan vain yhden pienen segmentin lähettämisen ilman kuittausta (ACK). Jos useampia pieniä segmenttejä muodostuu sillä välin, kun järjestelmä odottaa kuittausta edelliseen, ne liitetään yhteen suuremmaksi segmentiksi. Kaikki täysikokoiset segmentit lähetetään aina välittömästi, jos vastaanottajalla on riittävästi puskuritilaa. Algoritmin käyttö vähentää tehokkaasti vuorovaikutteisten sovellusten lähettämien pakettien määrää erityisesti hitailla yhteyksillä.

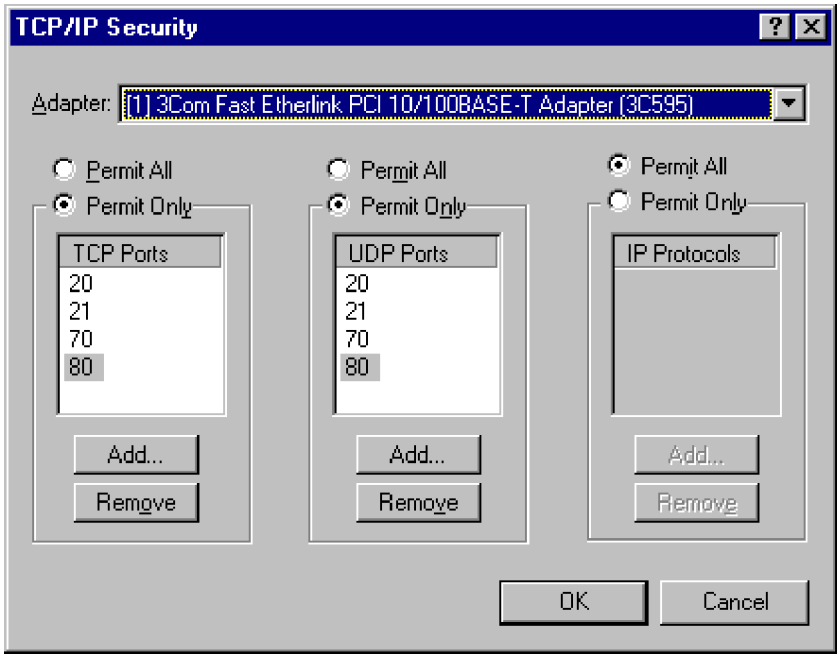
Windows Sockets -ohjelmat voivat poistaa Nagle-algoritmin käytöstä yhteyden ajaksi käyttämällä **TCP_NODELAY**-valitsinta. Kannattaa huomata, että vastaavasti verkkoliikenne kasvaa huomattavasti.

TCP/IP:n tietoturvasuotimet

Suodinten käyttö TCP/IP:n kanssa parantaa verkon tietoturvallisuutta, koska voidaan määritellä, millainen verkkoliikenne välitetään TCP/IP-pinossa ylempien kerrosten protokollille ja sovelluksille. Suodinten käyttö on yksi internet-palvelinten yleisimmistä tietosuojakeinoista.

TCP/IP:n turvallisuussuotimet kontrolloivat sitä, mihin portteihin tulevat TCP- ja UDP-yhteydet hyväksytään. Niiden avulla voit myös määritellä, mitä IP-protokollia on mahdollista käyttää.

Jos Windows NT -koneelle on määritelty TCP/IP-turvasuotimia, tulevat yhteyspyynnöt ja datagrammit hyväksytään tai hylätään niiden perusteella. Suotimet eivät vaikuta ulospäin suuntautuviin yhteyksiin (katso myös tarvittaessa kirjan lukua **3**).



Turvasuotimet määritellään erikseen jokaiselle **Adapter**-kohdassa valitulle verkkokortille, johon TCP/IP on sidottu. Saapuvan datan vertaaminen määriteltyihin suotimiin tehdään aina sen mukaan, mikä verkkosovitin vastaanottaa datan.

NetBIOS TCP/IP:n päällä

Windows NT:n NetBIOS over TCP/IP -toteutus NetBT käyttää seuraavia TCP- ja UDP-portteja:

- **UDP-portti 137** (nimipalvelut)
- **UDP-portti 138** (tietosähkepalvelut)
- **TCP-portti 139** (istuntopalvelut).

NetBIOS TCP/IP:n päällä määritellään RFC:issä 1001 ja 1002.

Windows NT:n **Netbt.sys**-laiteohjain on **ytimen** (*kernel*) komponentti, joka tukee **TDI** (*Transport Driver Interface*)-rajapintaa. Windows NT:n palvelin- ja työasemapalvelut käyttävät TDI:tä suoraan, ja **Netbt.sys**-ajuria käytetään muuntamaan perinteisten NetBIOS-sovellusten kutsut TDI-kutsuiksi. TDI:n käyttö NetBT-kutsuihin on ohjelmointiteknisesti vaikeampaa, mutta saattaa parantaa suorituskykyä ja vapauttaa ohjelmoijan NetBIOS:in historiallisista rajoituksista.

Suorituskyky

TCP on suunniteltu tarjoamaan paras mahdollinen suorituskyky hyvin erityyppisillä yhteyksillä. Käytännössä verkkoyhteyden suorituskykyyn vaikuttavat useat tekijät, mutta niistä tärkeimpiä ovat:

- Yhteysnopeus (montako bittiä sekunnissa yhteys kykenee välittämään)
- Levitysviiveet
- Ikkunan koko (paljonko kuittaamatonta dataa voi olla matkalla)
- Linkin luotettavuus
- Reitittimen ruuhkaisuus.

Seuraavassa on joitakin TCP:n suorituskykyyn vaikuttavia tekijöitä:

- Yhteysvälin kapasiteetti on yhtä suuri kuin (**kaistanleveys** * **edestakainen matka-aika**). Jos yhteys on luotettava, optimaalinen suorituskyky saadaan ikkunan koon ollessa suurempi tai yhtä suuri kuin yhteysvälin kapasiteetti. Suurin mahdollinen ikkunan koko on 65535, koska TCP-otsikko on 16-bittinen

- Välityskyky ei koskaan ylitä arvoa (**ikkunan koko** / **edestakainen matka-aika**)

- Jos linkki on epäluotettava tai pahoin ruuhkautunut ja paketteja putoilee, ikkunakoon suurentaminen ei välttämättä paranna suorituskykyä

- **Levitysviive** tai **johtumisviive** (*propagation delay*) riippuu valon nopeudesta, siirtolaitteiston viiveistä jne.

- **Siirtoviive** (*transmission delay*) riippuu verkkomedian siirtonopeudesta. Tietyn yhteyden **johtumisviive** on aina vakio, mutta **siirtoviive** riippuu paketin koosta. Alhaisilla nopeuksilla siirtoviiveestä muodostuu rajoittava tekijä. Suurilla nopeuksilla johtumisviiveestä tulee rajoittava tekijä.

Windows NT:n TCP/IP mukautuu useimpiin verkko-oloihin dynaamisesti ja tarjoaa automaattisesti parhaan mahdollisen yhteyskohtaisen suorituskyvyn. Yritykset säätää TCP/IP:n parametreja käsin johtavat usein suorituskyvyn heikkenemiseen, ellei datasiirron analysointiin ole käytettävissä asianmukaista laitteistoa ja pätevää verkkoasiantuntijaa.

User Datagram Protocol

User Datagram Protocol (UDP) on yhteydetön, epäluotettava siirtopalvelu. Sitä käytetään usein välitettäessä dataa yhdeltä lähettäjältä useille vastaanottajille broadcast- tai multicast-paketteina. Koska UDP-datagrammien perillemeno ei ole taattua, UDP:tä käyttävien ohjelmien tulee tarvittaessa varmistaa tiedonkulku omin neuvoin. Microsoft-verkoissa UDP:tä käytetään kirjautumiseen, selaamiseen ja nimenselvitykseen.

UDP ja nimiselvitys

UDP:tä käytetään nimiselvitykseen (*Name Resolution*) lähetettäessä viestejä NetBIOS-nimipalvelimelle (kuten WINS) tai aliverkon yleissanomaviestejä (*broadcast*) sekä DNS-nimien ja IP-osoitteiden selvitykseen.

NetBIOS-nimenselvitys käyttää UDP-porttia **137**. DNS-kyselyt käyttävät UDP-porttia **53**. Koska UDP itse ei takaa datagrammien perillemenoa, molemmat näistä palveluista käyttävät omia keinojaan tiedonkulun varmistamiseen.

Yleissanomien UDP-tietosähkeet eivät yleensä kulje IP-reititinten kautta, joten NetBIOS-nimiselvitys reititetyssä ympäristössä vaatii jonkinlaisen **nimipalvelimen** (WINS) tai **staattisen nimitietokannan** (LMHOSTS) käyttöä.

UDP ja mailslot-viestit

Useat NetBIOS-sovellukset käyttävät mailslot-viestejä. Toisen luokan mailslot on yksinkertainen mekanismi viestin lähettämiseksi yhdeltä NetBIOS-koneelta toiselle UDP:n yli. Mailslot-viestejä voidaan lähettää broadcastina koko aliverkkoon tai suoraan tietylle koneelle. Jos mailslot-viesti halutaan ohjata toiselle koneelle, käytettävissä täytyy olla jokin NetBIOS-nimenselvityskeino. Windows NT -palvelimella toimiva WINS-palvelu tarjoaa tällaisen keinon.

Transport Driver Interface

Microsoft kehitti **Transport Driver Interface** -rajapinnan (TDI) tarkoituksena tarjota suurempi joustavuus ja enemmän toimintoja kuin vanhoja rajapintoja (NetBIOS, Windows Sockets) käyttämällä oli mahdollista. TDI-rajapinta on kaikkien Windows NT:n siirtopalvelujen tarjoajien (*transport providers*) käytettävissä. TDI-määritys kuvailee primitiivifunktiot, joita tiedonsiirto-ohjaimet ja TDI-asiakkaat käyttävät kommunikointiin, sekä niiden kutsumekanismit. TDI-rajapinta toimii ainoastaan **ytimessä** (kernel).

Windows NT:n uudelleenohjaus- ja palvelinpalvelut käyttävät TDI:tä suoraan sen sijaan, että käyttäisivät välittävää NetBIOS-kerrosta. Tällä tavoin niiden on mahdollista kiertää useat NetBIOS:in rajoitukset, kuten 254 yhteyden raja.

TDI on ehkä kaikkein vaikein Windows NT:n verkko-ohjelmointirajapinnoista. Se on yksinkertaisesti välittävä kanava, joten ohjelmoijan on itse selvitettävä viestien formaatti ja tarkoitus.

Windows NT:n TDI-toteutukseen sisältyy:

- Tuki kaikille Windows NT:n verkkoprotokollille lukuun ottamatta DLC:tä
- Avoin nimeämis- ja osoitekäytäntö
- Viesti- (message) ja virtatyyppinen (stream) datasiirto
- Asynkroniset operaatiot
- Laajennettavuus
- Rajoitettu tuki standardeille ydintilan I/O-funktioille datan lähettämiseen ja vastaanottoon
- 32-bittiset osoitteet ja arvot.

Verkkosovellusrajapinnat

Verkkosovellukset voivat kommunikoida TCP/IP-pinon kautta useilla tavoilla. Osa niistä (kuten nimetyt putket, *Named Pipes*) kulkee työasemapalveluun (*Workstation*) kuuluvan **uudelleenohjauksen** (*redirector*) kautta.

Useat vanhemmat ohjelmat on kirjoitettu käyttäen NetBIOS-rajapintaa, jota puolestaan tukee **NetBIOS over TCP/IP**. Myös Windows Sockets -menetelmä on laajalti käytössä.

Windows Sockets -rajapinta

Windows Sockets on sovellusrajapinta (*Application Program Interface, API*), jota käytetään datan lähettämiseen ja vastaanottamiseen verkossa. Alunperin se suunniteltiin korkeimman tason liittymäksi TCP/IP-pinoihin, ja se tarjoaakin standardin Windows-rajapinnan useisiin erilaisiin siirtomenetelmiin, kuten TCP/IP ja IPX.

Windows Sockets -määrittelyn ohjelmointirajapinta perustuu Socket -rajapintaan, jonka syntypaikka oli **University of California at Berkeley**. Se sisältää joukon laajennuksia, jotka käyttävät hyväkseen Windowsin viestipohjaisuutta. Windows Sockets on avoin, käytännössä standardiksi muodostunut määritys, jonka alkuperäisistä kehittäjistä yksi on Microsoft.

Windows Sockets -ohjelmia on tarjolla runsaasti. Windows NT 4.0:ssa on käytössä 32-bittinen Windows Sockets -versio **2.0**. Aiemmat NT-versiot käyttivät 32-bittistä versiota **1.1**. Useat Windows NT:n mukana tulevat ohjelmat ovat Windows Sockets -pohjaisia, esimerkiksi **DHCP**-asiakas- ja palvelinsovellus.

Nimi- ja osoiteselvitys

Windows Sockets -ohjelmat käyttävät yleensä **gethostbyname()**-kutsua tietokoneen nimen tai IP-osoitteen selvittämiseen. Tällä kutsulla tehty selvityspyyntö etenee tyyppillisesti seuraavasti:

- Paikallisen tietokoneen nimen tarkistus
- Nimen etsiminen HOSTS-tiedostosta
- Jos DNS-palvelin on määritelty, haku DNS-palvelimelta
- Jos vastausta ei löydy, kutsutaan NetBIOS-nimenselvitystä.

Jotkin ohjelmat käyttävät **gethostbyaddr()**-kutsua, kun on tarve muuntaa **IP-osoite** tietokoneen nimeksi. Kutsu etenee seuraavasti:

- Paikallisen koneen nimen tarkistus
- Osoitteen etsiminen HOSTS-tiedostosta
- Jos DNS-palvelin on määritelty, haku DNS-palvelimelta
- Jos vastausta ei löydy, lähetetään NetBIOS:in tilapyyntö kyseessä olevaan IP-osoitteeseen. Jos vastaus löytyy, se tulkitaan ja siitä etsitään vastanneen tietokoneen nimi.

Windows Sockets -rajapintaa on laajennettu, jotta se tukisi IP-multicastingia. Laajennukset ja esimerkkiohjelmia on saatavilla Microsoftin ftp-palvelimelta.

Backlog-parametri

Windows Sockets -palvelinsovellukset luovat yleensä socketin ja käyttävät sitten **listen()**-komentoa jäädäkseen kuuntelemaan tulevia yhteyspyyntöjä. Yksi **listen()**-kutsun parametreista on backlog, jolla voidaan määritellä, kuinka monta yhteyspyyntöä ohjelma haluaa Windows Socketsin pitävän jonossa.

Windows NT Server 4.0 sallii **backlog**-maksimiarvon **200**. Kannattaa olla varovainen asetuksen suhteen, koska eräissä lähteissä väitetään ylärajan olevan *rajoittamaton*. NT:n työasemaversiossa maksimi on kuitenkin vain **5** yhteyspyyntöä.

Jos ftp- tai WWW-palvelin on hyvin vilkkaassa käytössä, arvon kasvattaminen saattaa parantaa suorituskykyä. **Microsoft Internet Information Server** sallii arvon muuttamisen rekisteriasetuksella:

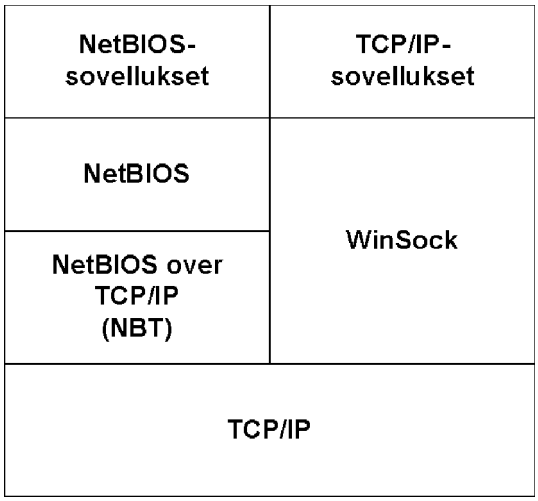
Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\InetInfo\Parameters**
Nimi	**ListenBackLog**
Tyyppi	**REG_DWORD**
Arvo	**1 - rajoittamaton; oletus 15**

Asetusta **50** pidetään hyvänä **kovassa käytössä** olevissa IIS-palvelimissa.

NetBIOS-rajapinta

NetBIOS (*Network Basic Input/Output System*) on itse asiassa ohjelmarajapinta ja nimeämiskäytäntö, ei protokolla. IBM:n vuonna 1985 määrittelemä NetBEUI-protokolla on tarkoitettu ohjelmille, jotka käyttävät NetBIOS-rajapintaa. NetBEUI on kuitenkin kevyt protokolla, eikä se reititysominaisuuksien puuttuessa sovellu keskisuuriin tai suuriin verkkoihin.

NetBIOS over TCP/IP (NetBT, myös lyhennettä NBT käytetään) puolestaan tarjoaa ohjelmointirajapinnan TCP/IP-protokollaan ja laajentaa näin NetBIOS-asiakas/palvelin-ohjelmoinnin mahdollisuuksia laajaverkkoihin sekä tarjoaa yhteensopivuuden useiden käyttöjärjestelmien kesken. Seuraava kuva selventää NetBT:n ja NetBIOS:in suhdetta:



Windows NT:n seuraavat palvelut käyttävät NetBT:tä suoraan TDI:n kautta:

- Workstation-työasemapalvelu
- Server-palvelinpalvelu
- Browser-selauspalvelu
- Messenger-viestinvälityspalvelu
- Netlogon-kirjautumispalvelut.

Windows NT:hen sisältyy myös NetBIOS-emulaattori, joka muuntaa standardit NetBIOS-kutsut vastaaviksi TDI-kutsuiksi.

NetBIOS-nimet ja nimiselvitys

Jotta Windows NT:ssä voitaisiin NetBIOSin yhteydessä käyttää TCP/IP:tä, on määritettävä tietokoneen verkkotunnukset, jotka ovat **tietokoneen nimi** (esimerkiksi PC-JKI) ja sen **IP-osoite** (esimerkiksi 193.88.121.65). Viimeksi mainittu tietokoneen IP-osoite on kyseisen tietokoneen yksilöllinen tunnus TCP/IP-verkossa (tämän lisäksi TCP/IP:ssä ja Internetissä tietokoneen nimessä on **DNS-toimialueen** (*domain*) tunnus, esimerkiksi **VERSTAS.COM**).

Paikallisessa verkossa voidaan yleensä käyttää vain tietokoneen nimeä, esimerkiksi **PC-JKI**. Vaikka tietokoneet tunnistavat toisensa konekohtaisten IP-osoitteiden perusteella, käyttäjät käyttävät yleensä mieluummin tietokoneiden nimiä - esimerkiksi **LUOKKA2** lienee helpompi muistaa kuin **139.28.11.97**. Siksi TCP/IP-verkoissa tarvitaan menetelmä, jolla tietokoneiden NetBIOS-nimet muunnetaan IP-osoitteiksi.

NetBIOS-nimiavaruus on yksiulotteinen, joten jokaisen verkkonimen täytyy olla yksilöllinen. NetBIOS-nimien maksimipituus on 16 merkkiä. Resurssien tunnistamiseen käytetään NetBIOS-nimiä, jotka rekisteröidään dynaamisesti aina tietokoneen käynnistyessä, palvelun käynnistyessä tai käyttäjän kirjautuessa sisään. Nimet voidaan rekisteröidä joko **yksilöllisinä** (yksi omistaja) tai **ryhmäniminä** (useita omistajia). Resurssin paikantamiseen tai nimen muuntamiseen IP-osoitteeksi käytetään

NetBIOS-nimikyselyä.

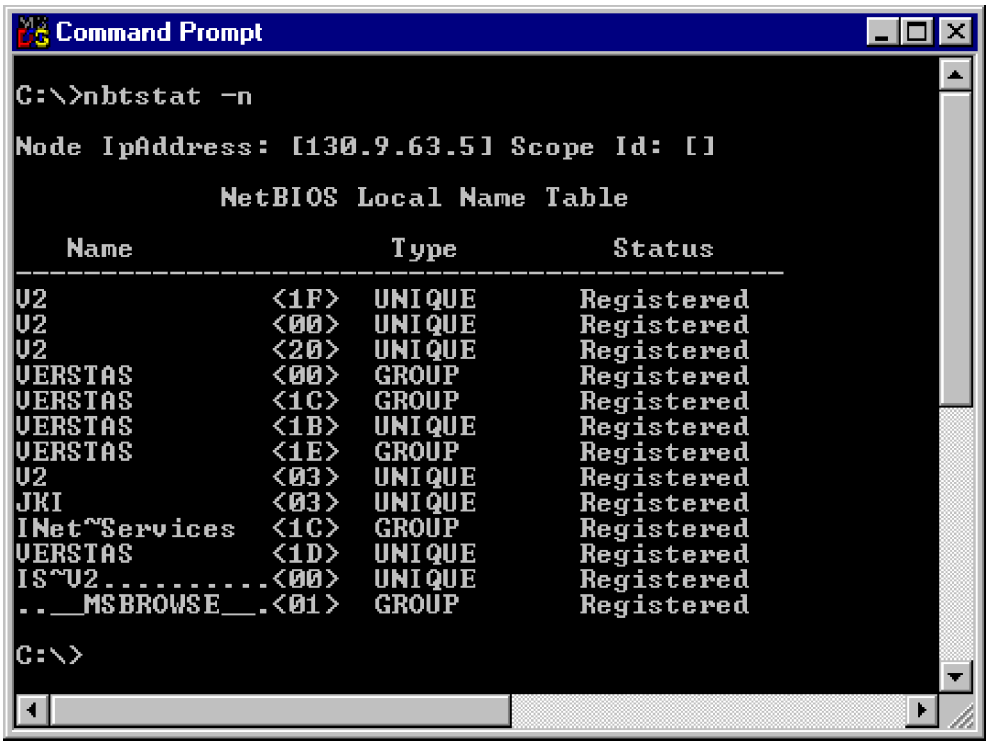
Microsoftin verkkokomponentit, kuten NT:n työasema- ja palvelinpalvelut, sallivat käyttäjän määritellä ensimmäiset 15 NetBIOS-nimen merkkiä, mutta varaavat viimeisen (16.) merkin resurssityypin ilmaisemiseen (heksa-arvo 00-FF).

NT-koneen NetBIOS-nimi on annettu asennuksen yhteydessä (Computername). Se on toki myös rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control**
Nimi	**Computername**
Tyyppi	**REG_SZ**
Arvo	**NT-koneen nimi**

Voit selvittää tietokoneesi oman ja muut käytössä olevat NetBIOS-nimet komennolla

nbtstat -n



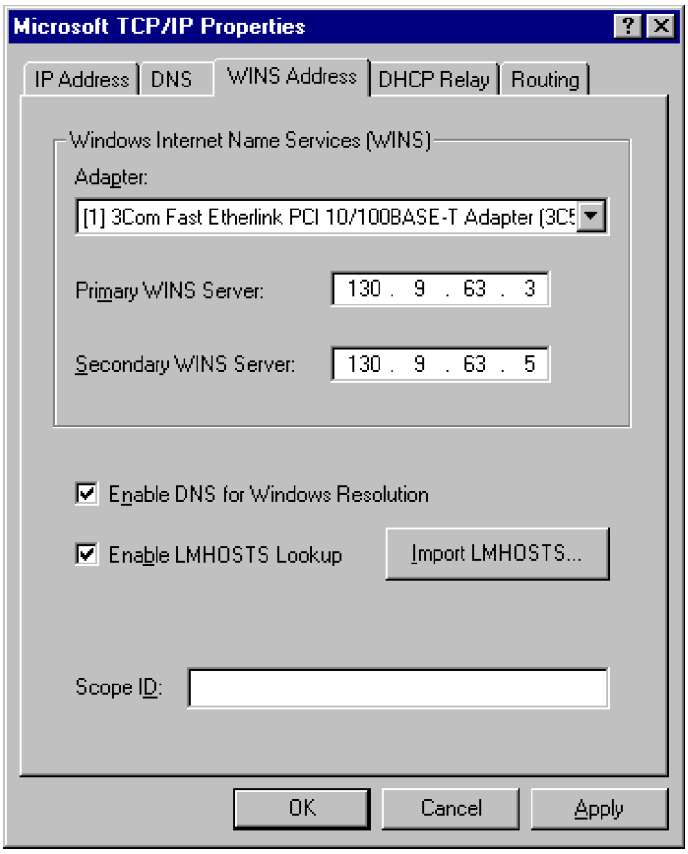
Seuraavassa luettelo **NetBIOS**-nimistä:

\\työaseman_nimi[00h]	Työasema (Workstation)-palvelulle rekisteröity nimi. Ylläolevassa esimerkissä **V2[00h]**
\\työaseman_nimi[03h]	Sanomanvälitys (Messenger)-palvelulle rekisteröity työaseman nimi
\\työaseman_nimi[BEh]	Verkkomonitori (jos käynnistetty)
\\työaseman_nimi[1Fh]	NetDDE (jos käynnistetty)
\\työaseman_nimi[20h]	Palvelin (Server)-palvelulle rekisteröity nimi
\\toimialue[00h]	Toimialueen nimi; työasema pystyy ottamaan vastaan LAN Manager-tyyppisiä yleissanomia
\\toimialue[1Bh]	Toimialueen nimi; ohjauskoneen (PDC) rekisteröimä nimi, ja kyseinen ohjauskone toimii *Domain Master Browserina*. Kun kyseistä toimialuetta selataan, WINS osaa palauttaa tämän nimen rekisteröineen palvelimen nimen
\\toimialue[1Ch]	Toimialueen nimi; ohjauskoneiden (BDC) rekisteröimä nimi, jolla ne etsivät verkosta PDC:n
\\toimialue[1Dh]	Toimialueen pääselaaja (*Master Browser*)
\\toimialue[1Eh]	Toimialueen pääselaajan (*Master Browser*) vaalissa (*Election*) käytetty nimi
\\--__MSBROWSE__[01h]	Selauspalvelu
\\käyttäjätunnus[03h]	Tällä hetkellä työasemaan kirjoittautunut käyttäjä. Ylläolevassa esimerkissä esimerkiksi **JKI[03h]**. Tällöin voidaan lähettää viesti esimerkiksi komennolla **NET SEND käyttäjä viesti**

NetBIOS Scope

NetBIOS Scope tunnetaan myös nimellä TCP/IP Scope, ja se on menetelmä toisen elementin lisäämiseksi yksielementtiseen tietokoneen NetBIOS-nimeen. Scope ID on merkkijono, joka lisätään NetBIOS-nimeen ja jota käytetään koneen NetBT-kommunikaatiossa. Merkkijono voi olla myös monisainen, esimerkiksi **palvelin.yritys.fi**. NetBIOS Scopen käyttöönottoa ei suositella, ellei se jo ole käytössä organisaatiossasi, tai jos verkossasi on käytössä DNS.

Oletusarvoisesti NetBIOS Scopen arvo on NULL. Voit muuttaa oletusta verkkoasetusten WINS Address -välilehden kohdasta Scope ID.



NetBIOS-nimen ja NetBIOS Scopen yhteenlaskettu pituus ei saa ylittää 256 merkkiä.

NetBIOS Scopen vaikutus käytännössä on, että jos se on muuta kuin NULL, se eristää omaksi ryhmäkseen ne tietokoneet, joilla on sama Scope ID. Nämä tietokoneet voivat siis viestiä vain keskenään. Käytä siis NetBIOS Scopea ainoastaan, jos haluat eristää osan verkossa olevista tietokoneista omaksi ryhmäkseen, jonka kanssa muut tietokoneet eivät

saa viestiä.

Kun NetBIOS Scope on asetettu, se liitetään automaattisesti kaikkiin tietokoneen lähettämiin NetBIOS-viesteihin. Toisin sanoen, jos tietokoneilla A ja B on eri NetBIOS Scope, niillä käynnistetyt NetBIOS-sovellukset eivät pysty viestimään keskenään:

- Windows NT- ja Windows 95 -koneet samalla NT-toimialueella kykenevät viestimään keskenään **vain** jos niillä on **sama** NetBIOS Scope ID

- Käyttäjätietojen varmennusta ei kuitenkaan voida suorittaa toimialueiden välillä, jos toimialueilla on eri NetBIOS Scope ID (rikkoo luottosuhteen)

- Käyttäjät eivät pysty kirjautumaan toimialueelle Windows NT Workstation- ja Windows 95 -koneista, jos työaseman NetBIOS Scope ID eroaa käyttäjän toimialueen ohjauskoneiden Scope ID:stä

- Käyttäjät eivät pysty kirjautumaan millekään koneelle, jonka Scope ID eroaa valitun toimialueen ohjauskoneiden Scope ID:stä

- Käyttäjät eivät pysty muodostamaan verkkoyhteyttä palvelimeen, jonka Scope ID eroaa käyttäjän palvelinalueen ohjauskoneen Scope ID:stä.

Useat Windows NT -sovellukset, kuten verkkoon kirjautuminen ja ohjauskoneiden kirjautumisen välitys käyttävät NetBIOS-nimiä. Harkitse siis tarkoin, ennen kuin muutat NetBIOS ID:n oletusarvoa.

NetBIOS Scope on täysin eri asia kuin **DHCP Scope**, mitä käytetään määrittelemään, miltä väliltä DHCP-palvelin voi jakaa osoitteita asiakkaiden käyttöön.

NetBT-yhteydet

NetBT-yhteys muodostetaan kahden koneen (tai nimen) välille. Jos esimerkiksi Windows NT -työasema pyytää yhteyttä palvelimella olevaan jaettuun tiedostoon, käydään läpi seuraavat vaiheet:

1) Palvelimen NetBIOS-nimi muunnetaan IP-osoitteeksi

2) TCP-yhteys muodostetaan työasemalta palvelimelle käyttäen porttia **139**

3) Työasema lähettää NetBIOS-yhteyspyynnön palvelimelle TCP-yhteyden yli. Jos palvelin kuuntelee, se vastaa, ja yhteys muodostuu.

Kun NetBIOS-yhteys on muodostettu, työasema ja palvelin neuvottelevat korkeamman tason protokollan, jota yhteyden aikana käytetään. Microsoft-verkoissa käytetään aina ainoastaan yhtä NetBIOS-yhteyttä kerrallaan kahden NetBIOS-nimen välillä. Yhteyden muodostamisen jälkeen kaikki pyynnöt käyttävät samaa yhteyttä.

NetBIOS:in keepalive-viestejä käytetään joka yhteyden aikana varmistamaan, että molemmat tietokoneet ovat edelleen kunnossa ja pystyvät pitämään yhteyttä yllä. Jos siis esimerkiksi työasema kaatuu yllättäen kesken yhteyden, palvelin osaa lopettaa yhteyden siististi - sama pätee toisinkin päin. NetBIOS:in keepalive-viestejä lähetetään rekisteriparametrin **SessionKeepAlive** mukaisesti. Oletusarvo on kerran tunnissa.

Jos käytetään LMHOSTS-tiedostoja, ja tiedostossa on **virheellinen palvelimen nimi**, saattaa yhteys palvelimeen onnistua oikealla IP-osoitteella mutta väärällä nimellä. Tässäkin tapauksessa TCP-yhteys muodostetaan, mutta palvelin torjuu NetBIOS-yhteyspyynnön, koska pyynnössä on väärä nimi ja palvelin ei kuuntele tuolle nimelle osoitettuja pyyntöjä.

Tuloksena on

Error 51: Remote computer not listening.

NetBT-tietosähkepalvelut

Tietosähkeitä lähetellään NetBIOS-koneelta toiselle portin **138** kautta. Tietosähkepalvelun avulla viestin voi lähettää joko yhdelle vastaanottajalle tai vastaanottajaryhmälle. Ryhmälähetys voi kohdistua joko useaan IP-osoitteeseen tai yleissanomana kaikille.

Esimerkiksi komento

NET SEND /D:Verstas Palvelin ajetaan kohta alas

lähettäisi viestin ryhmänimelle **Verstas[03]**, joka puolestaan muunnettaisiin aliverkon IP-broadcastiksi. Tällöin joten lähtevällä tietosähkeellä olisi seuraavat ominaisuudet:

- Kohteen MAC-osoite: broadcast (255.255.255.255)
- Lähettäjän MAC-osoite: lähettävän verkkokortin osoite
- Kohteen IP-osoite: paikallisen aliverkon broadcast-osoite
- Lähettäjän IP-osoite: lähettäjäkoneen IP-osoite
- Kohteen nimi: Verstas[03] (etäkoneiden Messenger-palvelu)
- Lähettäjän nimi: työasema[03] (lähettävän tietokoneen Messenger-palvelu)

Kaikki tietokoneet samassa aliverkossa vastaanottaisivat tietosähkeen, ja vähintään UDP-protokolla käsittelisi sen. Jos tietokoneella olisi käytössä NetBIOS, UDP välittäisi datagrammin NetBT:lle portiin **138**. NetBT tarkistaisi kohteen nimen ja välittäisi datagrammin edelleen ylöspäin.

NetBIOS-nimien rekisteröinti ja selvitys

Windows NT:n versiot 3.5x ja 4.0 käyttävät useita menetelmiä NetBIOS-resurssien paikantamiseen:

- NetBIOS-nimien välimuisti
- NetBIOS-nimipalvelimet
- Aliverkon IP-yleissanoma (*broadcast*)
- Staattiset LMHOSTS-tiedostot
- Staattiset HOSTS-tiedostot
- DNS-palvelimet.

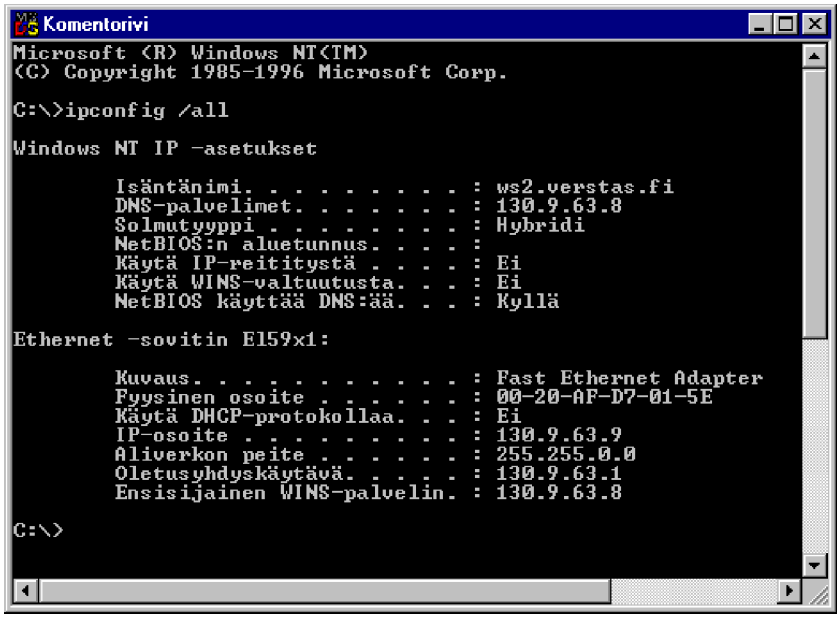
Aiemmat NT-versiot käyttivät vain välimuistia, yleissanomia ja LMHOSTS-tiedostoja. Windows NT:n versioissa 3.5x ja 4.0 käytössä on kuitenkin NetBIOS-nimipalvelu WINS, ja järjestelmään tehtiin muutoksia jotta NetBIOS-sovellukset voisivat tehdä DNS-kyselyjä lisäämällä NetBIOS-nimen perään erikseen määriteltävän palvelinalueen päätteen.

Komennolla **NBTSTAT** voi tarkkailla nimivälimuistia:

- **NBTSTAT -R** lataa uudelleen **LMHOSTS**-tiedoston
- **NBTSTAT -r** kertoo tilastotiedot nimiselvityksestä
- **NBTSTAT -c** kertoo nimivälimuistissa olevat nimet.

Solmutyyppi

Solmu (node) on mikä tahansa viestivä verkon komponentti. Solmun tyyppi määrittelee käytettyjen nimiselvitysmenetelmien käyttöjärjestyksen.



Solmutyypin näet **IPCONFIG /ALL**-komennolla. Se voi olla jokin seuraavista:

- B-node (*broadcast*) - käyttää vain yleissanomia (broadcast) nimiselvitykseen ja rekisteröintiin
- P-node (*point-to-point*) - käyttää vain NetBIOS-nimipalvelimelle (tässä tapauksessa WINS-palvelimelle) tehtäviä point-to-point-nimikyselyitä nimien rekisteröintiin ja selvitykseen
- M-node (*mixed*) - nimiselvitys ensin yleissanomalla (B-node), jos vastausta ei tule, sitten P-node-tyyppisesti. Tämä ei ole hyvä ratkaisu isoissa verkoissa yleissanomien määrän vuoksi
- H-node (*hybrid*) - käyttää P-nodea sekä rekisteröintiin että selvitykseen. Jos nimipalvelinta ei kuitenkaan löydy, vaihtaa B-node-tyyppisiin kyselyihin. Jatkaa nimipalvelimen etsimistä ja vaihtaa takaisin P-node-tyyppiseen käytäntöön, jos palvelin löytyy. Tämä on hyvä ratkaisu
- Microsoft Enhanced Käyttää tavallisten tyyppien lisäksi pai-

kallista **LMHOSTS**-tiedostoa, WINS-proxyä sekä Windows Sockets -kutsua **gethostbyname()** (joka puolestaan käyttää standardia DNS-selvitystä sekä paikallista HOSTS-tiedostoa).

Näistä vaihtoehdoista on joskus vaikea päättää, mitä menetelmää pitäisi käyttää ja missä järjestyksessä kukin konfiguraatio käyttää nimipalveluita.

Windows NT:n palvelinversion mukana tuleva NetBIOS-nimipalvelinohjelmisto on nimeltään **Windows Internet Name Service** (WINS). Useimmat WINS-asiakkaat ovat H-node-tyyppisiä: ne yrittävät ensin rekisteröidä ja selvittää nimiä WINS-palvelun kautta, ja jos se epäonnistuu, sitten paikallisella aliverkon yleissanomalla. Nimipalvelimen käyttö on yleisesti ottaen parempi vaihtoehto kahdesta syystä:

- Reitittimet eivät yleensä välitä broadcast-viestejä eteenpäin
- Yleissanoma menee aliverkon jokaiselle tietokoneelle ja vaatii näin joka tietokoneelta prosessointiaikaa.

Jos työasema käyttää WINS-palvelua, oletustyyppi on **H-node**. Asetus voidaan antaa myös DHCP:n avulla, se on **046 WINS/NBT node type** (*NetBIOS over TCP/IP*-solmun tyyppi).

Solmun tyyppi voidaan määritellä rekisteriin:

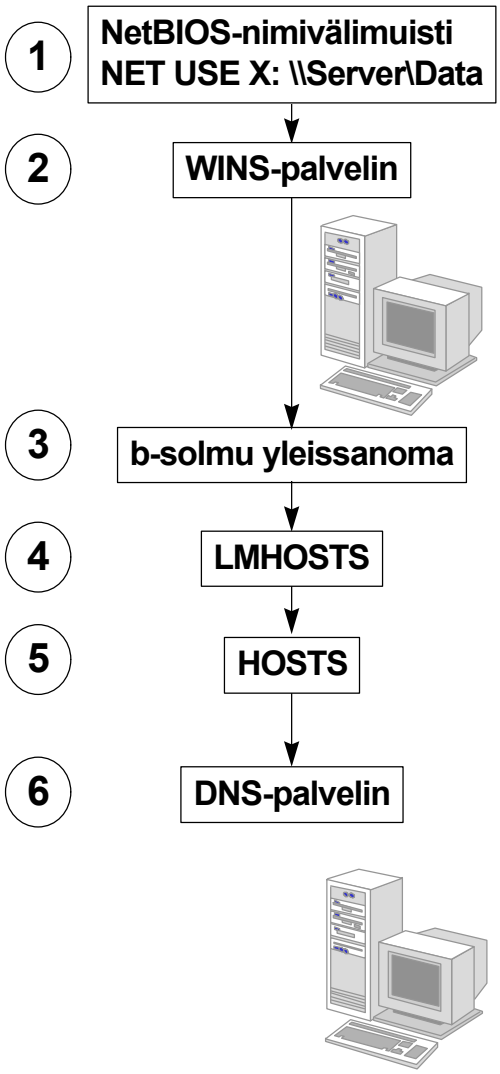
Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**CurrentControlSet\Services\NetBT\Parameters**
Nimi	**NodeType**
Tyyppi	**REG_DWORD**
Arvo	**1 = B-node (*broadcast*)** **2 = P-node (*point-to-point*)** **4 = M-node (*mixed*)** **8 = H-node (*hybrid*)**

Jos nimeä ei ole, käytetään oletuksena 1 tai 8 riippuen WINS:in käytöstä.

Asetus voidaan antaa myös DHCP:n avulla, mutta jos nimenomaan on

annettu myös NodeType, niin se ohittaa DHCP:n avulla annetun solmutyypin.

H-solmun (H-node) nimiselvitys etenee seuraavasti:



1) Ensin tutkitaan nimivälimuisti
2) Ohjataan kysely WINS-palvelimelle
3) Lähetetään yleissanoma
4) Tutkitaan LMHOSTS (jos **Käytä LMHOSTS-hakua** on valittu)
5) Tutkitaan HOSTS (jos **Käytä DNS:ää Windows nimiselvityksessä** on valittu)
6) Ohjataan lopuksi kysely DNS-palvelimelle.

Nimiselvitys usean verkkokortin tapauksessa

NetBT muodostaa sidoksen ainoastaan yhteen IP-osoitteeseen yhtä verkkosovitinta kohti. NetBT:n näkökulmasta tietokone on siis *multihomed* ainoastaan silloin, kun siinä on useampia kuin yksi verkkokortti. Kun rekisteröintipaketti lähtee moniverkkokorttiselta tietokoneelta, siihen liitetään tunniste *multihomed name registration*, niin ettei saman nimen rekisteröinnistä usealle verkkoverkotille synny ristiriitaa.

Kun tällainen tietokone vastaanottaa yleissanoma-nimikyselyn, kaikki NetBT-sidokset vastaavat omalla osoitteellaan, ja oletusarvoisesti asiakas valitsee ensimmäisen vastauksen mukaisen osoitteen ja ottaa yhteyden siihen. Tätä käytäntöä voi kontrolloida rekisteriparametrilla **RandomAdapter**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**CurrentControlSet\Services\NetBT\Parameters**
Nimi	**RandomAdapter**
Tyyppi	**REG_DWORD**
Arvo	**0 (oletus) tai 1; arvolla 1 NetBT valitsee satunnaisesti palauttamansa IP-osoitteen nimikyselyssä**

Toinen asetus on **SingleResponse**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**CurrentControlSet\Services\NetBT\Parameters**
Nimi	**SingleResponse**
Tyyppi	**REG_DWORD**
Arvo	**0 (oletus) tai 1; arvolla 1 NetBT palauttaa vain yhden IP-osoitteen nimikyselyssä (ja RandomAdapter-asetus toimii)**

Kun WINS-palvelin saa suoran nimikyselyn, se vastaa oletuksena luettelemalla kaikki IP-osoitteet, jotka moniverkkokorttinen tietokone on rekisteröinyt WINS-palveluun.

Parhaan IP-osoitteen valitseminen tarjotuista vaihtoehdoista on asiakkaan tehtävä. Tässä käytetään seuraavaa algoritmia:

- Jos jokin löytyneistä IP-osoitteista kuuluu samaan aliverkkoon kuin kyselyn lähettänyt NetBT-sidos, kyseinen osoite valitaan. Jos useampi kuin yksi osoite täyttää tämän ehdon, yksi osoitteista valitaan satunnaismenetelmällä
- Jos jokin löytyneistä IP-osoitteista kuuluu samaan aliverkkoon kuin mikä tahansa kysyvän tietokoneen NetBT-sidos, kyseinen osoite valitaan. Jos useampi kuin yksi osoite täyttää tämän ehdon, yksi osoitteista valitaan satunnaismenetelmällä
- Jos yksikään löytyneistä osoitteista ei kuulu samaan aliverkkoon kuin jokin kysyvän tietokoneen NetBT-sidos, jokin osoitteista valitaan satunnaismenetelmällä.

Tämän algoritmin avulla saadaan suorat yhteydet pidettyä etusijalla, ja samalla yhteyspyynnöt saadaan melko jaettua tietokoneen eri verkkosovittimien kesken.

Windows NT:n Workstation- ja Server-palvelut

Windows NT käyttää Workstation- ja Server-palveluita tiedostojen ja tulostimien jakamiseen. Molemmat palvelut keskustelevat NetBIOS over TCP/IP:n avulla, vaikka eivät olekaan NetBIOS-sovelluksia. Nämä palvelut kommunikoivat suoraan NetBT:n kanssa käyttäen TDI-rajapintaa. Koska ne ovat TDI-asiakkaita, ne ovat tehokkaita eivätkä niitä koske NetBIOS-rajoitukset, kuten 254 yhteyden raja. **Server Message Block** (SMB) -protokollaa käytetään komentojen ja vastausten lähettämiseen asiakkaiden ja palvelinten välillä. SMB-määritys on julkinen ja saatavilla Microsoftin ftp-palvelimelta.

Kun käyttäjä kirjautuu Windows NT -toimialueelle, käydään läpi seuraava tapahtumasarja:

- Jos tietokone käyttää WINS:ää, se lähettää WINS-palvelimelle NetBIOS-nimikyselyn nimestä **toimialue[1C]**

- WINS-palvelin vastaa lähettämällä korkeintaan 25 IP-osoitetta, joista kukin vastaa jotakin toimialueen domain controlleria. Yksi osoitteista on aina **ensisijainen ohjauskone** (Primary Domain Controller)

- Paikalliseen aliverkkoon lähetetään pyyntö **\MAILSLOT\NET\NTLOGON**. Jos tähän yleissanomaan saadaan vastaus, järjestelmä ottaa yhteyden vastanneeseen ohja ja yrittää kirjautumista

- Muussa tapauksessa kirjautumisprosessi lähettää datagrammin suoraan jokaiseen WINS-vastauksessa olleeseen IP-osoitteeseen ja yrittää kirjautumista siihen ohjauskoneeseen, joka vastaa ensimmäisenä

Kaikki verkon ohjauskoneet rekisteröivät nimen **toimialue[1C]**, yleensä WINS-tietokantaan. Kaikki salasanatiedot muunnetaan salakirjoitukseksi ennen niiden siirtämistä verkossa.

Yhteyksien muodostaminen verkkoresursseihin

Kun työasema yrittää ottaa yhteyttä verkossa olevaan jaettuun resurssiin, kyseistä resurssia kutsutaan sen NetBIOS-nimellä. Nimen muuntaminen IP-osoitteeksi tehdään edellä kuvatulla tavalla.

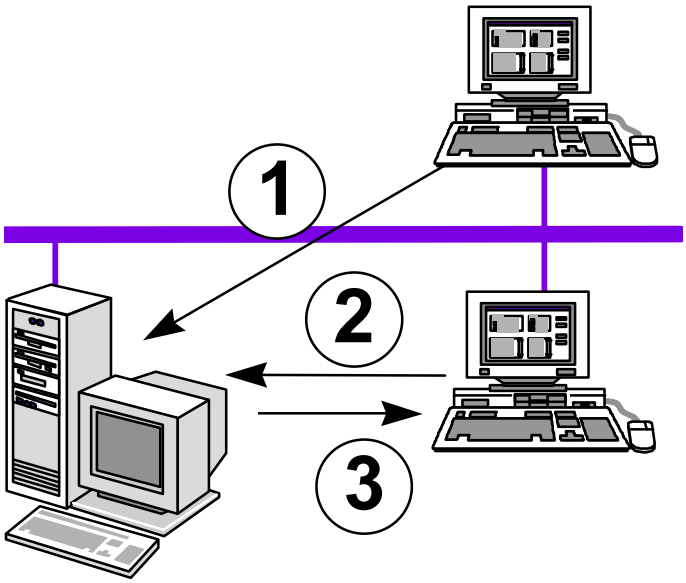
Kun kohdekoneen IP-osoite on tiedossa, muodostetaan tavanomainen TCP/IP-yhteys ja sen päälle NetBIOS-yhteys. Käyttäjätunnistus tapahtuu salakirjoitettuja salasanoja käyttäen, ja sen jälkeen asiakas/palvelinviestejä vaihdetaan SMB-protokollan avulla. Työasema ja palvelin käyttävät kehittyneitä menetelmiä suorituskyvyn kasvattamiseksi ja verkkoliikenteen pitämiseksi mahdollisimman pienenä. Kun käytetään WINS:ää, IP-yleissanomiin ei tarvitse turvautua (ainoana poikkeuksena **ARP**).

WINS

Windows NT -palvelimen **WINS** (*Windows Internet Name Service*)-palvelun avulla voidaan määritellä työasemien/palvelimien NetBIOS-nimet keskitetysti.

WINS (*Windows Internet Name Service*) on laajennettu NetBIOS-nimipalvelin (*NetBIOS Name Server*, NBNS), jonka tarkoitus on vähentää B-tyypin solmujen nimiselvitykseen käyttämiä yleissanomia verkossa, ja siten helpottaa ja nopeuttaa nimiselvitystä sekä keventää verkon kuormitusta. Koska WINS toimii dynaamisesti, tieto on aina ajantasalla. WINS on laajennus RFC 1001 ja RFC 1002 -määrityksiin.

Toimintaperiaate



Ennen kuin kaksi NetBIOS-konetta voi keskustella, kohdekoneen IP-osoite on selvitettävä, koska TCP/IP ei toimi NetBIOS-nimien avulla. Tämä etenee seuraavasti:

1) Kun WINS-asiakas käynnistyy (olipa se NT-palvelin tai Työryhmä-Windows-työasema), se rekisteröi NetBIOS-nimensä ja IP-osoitteensa määritellylle WINS-palvelimelleen

2) Kun WINS-asiakas haluaa kohteen nimiselvitystä, se kysyy tietoja määritellyltä WINS-palvelimeltaan (ensin tarkastetaan oma NetBIOS-nimivälimuisti). Jos ensisijainen (Primary) WINS-palvelin ei vastaa, asiakas kokeilee vielä kaksi kertaa ja vaihtaa sitten toissijaiseen (Secondary) WINS-palvelimeen

3) Jos WINS-palvelin löytää NetBIOS-nimen/IP-osoitteen, se palauttaa kohteen IP-osoitteen WINS-asiakkaalle. Koska WINS toimii dynaamisesti, tieto on aina ajantasalla. Jos nimeä ei löydy, WINS-palvelin palauttaa asiakkaalle sanoman *Requested name does not exist* ja asiakas saattaa siirtyä käyttämään B-tyypin nimiselvitystä (yleissanoma). Nimi voi löytyä LMHOSTS- tai HOSTS-tiedostosta tai DNS:n avulla.

Huomattavaa:

- Jo yksi WINS-palvelinkin saattaa olla riittävä, mutta kaksi WINS-palvelinta takaa vikasietoisuuden, koska WINS-palvelimet voivat välittää omia osoitetietojaan toisille WINS-palvelimille. Nimiselvityspyynnöt ovat osoitteellisia tietosähkeitä, joita voidaan reitittää

- Jotta nimet siirtyisivät myös vanhemmissa verkoissa, a.o. verkossa pitää tarvittaessa olla **yksi** WINS Proxy-agentti

- LAN Manager-koneet eivät tue WINS:iä rekisteröinnissä, mutta nimiselvityksessä kylläkin. Näiden tietokoneiden NetBIOS-nimille on määriteltävä staattinen osoite

- Kahden samannimisen tietokoneen tapauksessa WINS lähettää ensin rekisteröityneelle haasteen kolme kertaa 500 millisekunnin välein. Jos vastausta ei tule, uusi samanniminen saa nimen käyttöönsä. Jos kyseessä on **moniosoitteinen** (*multihomed*) tietokone, jokainen IP-osoite käydään läpi

- WINS käyttää UDP-porttia **137** (*NetBIOS Name Service*)

- Työasemassa pitää määritellä ensisijaisen WINS-palvelimen IP-osoite, toissijaisen määrittely on valinnainen.

WINS-palvelimen käyttöönotto

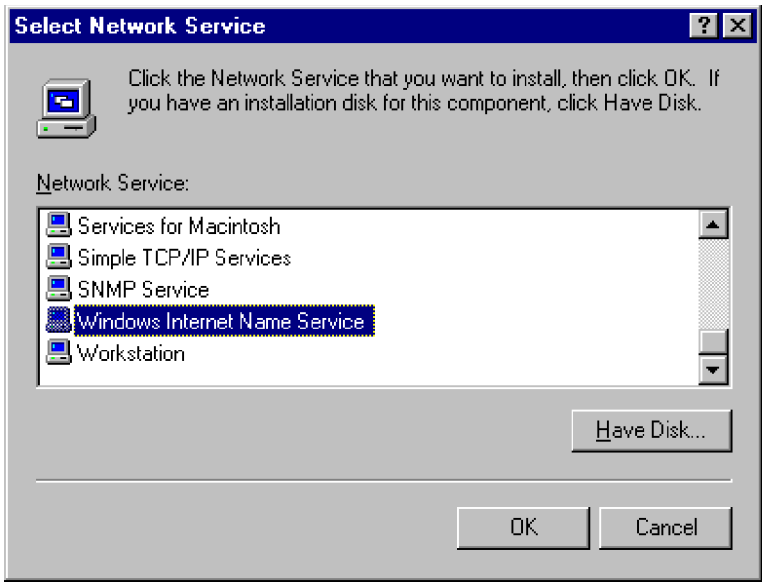
WINS-palvelimen käyttöönoton edellytykset ovat:

- Windows NT-palvelin (ei tarvitse olla ohjauskone)
- TCP/IP-asetukset (staattinen IP-osoite, aliverkon peitto ja oletusyhdyskäytävä).

Työasemat voivat olla:

- Windows NT Server 3.5x - 4.0
- Windows NT Workstation 3.5x - 4.0
- Työryhmä-Windows 3.11 (Windows for Workgroups 3.11 Windows NT Serverin CD-ROM-version MS TCP/IP-32b:llä)
- Windows 95
- Microsoft Network Client 3.0 for DOS (Windows NT Serverin CD-ROM-version TCP/IP:llä)
- LAN Manager 2.2c for MS-DOS (Windows NT Serverin CD-ROM-versio; OS/2-versio ei tuettu)
- Työasemassa on määriteltävä ensisijaisen WINS-palvelimen osoite tai sekä ensi- että toissijaisen WINS-palvelimen osoite.

WINS asennetaan Windows NT 4.0 -palvelimessa käyttöön Ohjauspaneelin **Network** -kuvakkeella valitsemalla **Services**-välilehdessä **Add** ja selaamalla kohteeksi **Windows Internet Name Service**.



Asennuksen jälkeen voit hallita WINS-palvelua **WINS Manager**-valvontaohjelmalla joko paikallisesti palvelimessa tai Windows 95/Windows NT 4.0-työasemasta, johon olet asentanut palvelimien valvontaohjelmat.

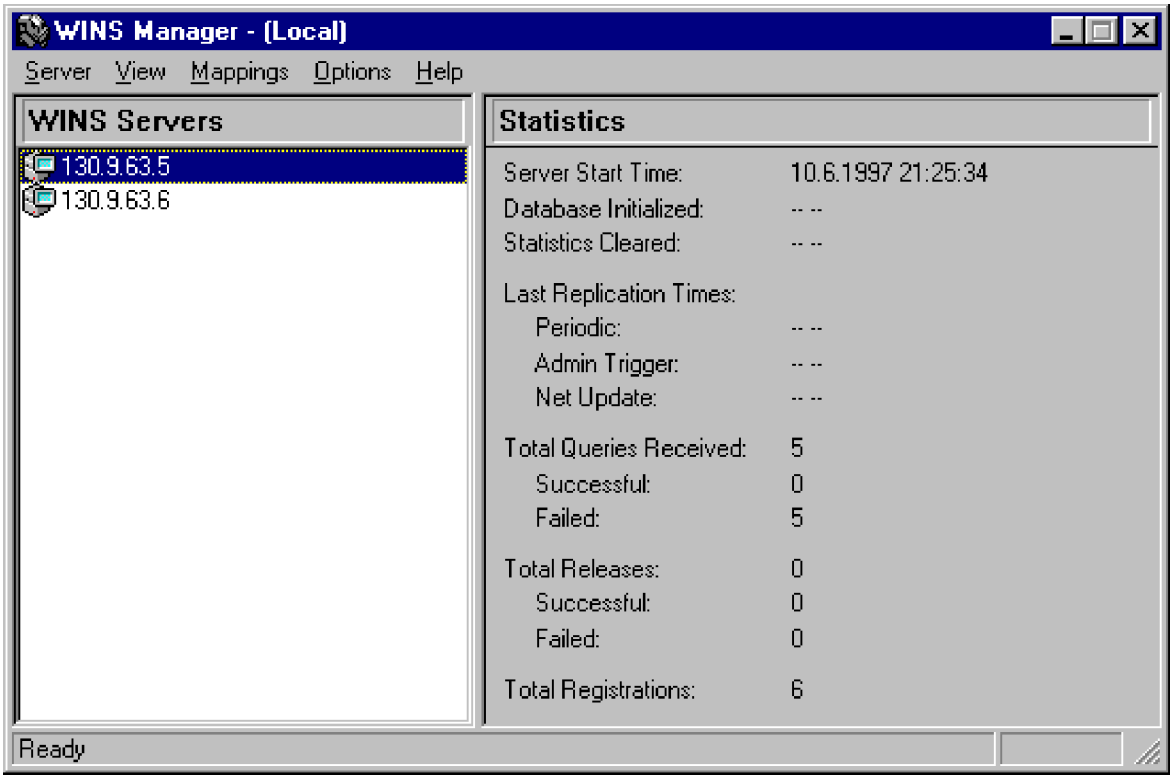
Kannattaa vaikkapa tehdä pikakuvake **WINSADMN.EXE**-ohjelmalle, se löytyy **Winnt\System32**-kansiosta. Voit myös valvoa toista WINS-palvelinta toisesta WINS-palvelimesta.

Muista myös tarkkailla WINS-palvelimen tapahtumalokia Event Viewerillä.

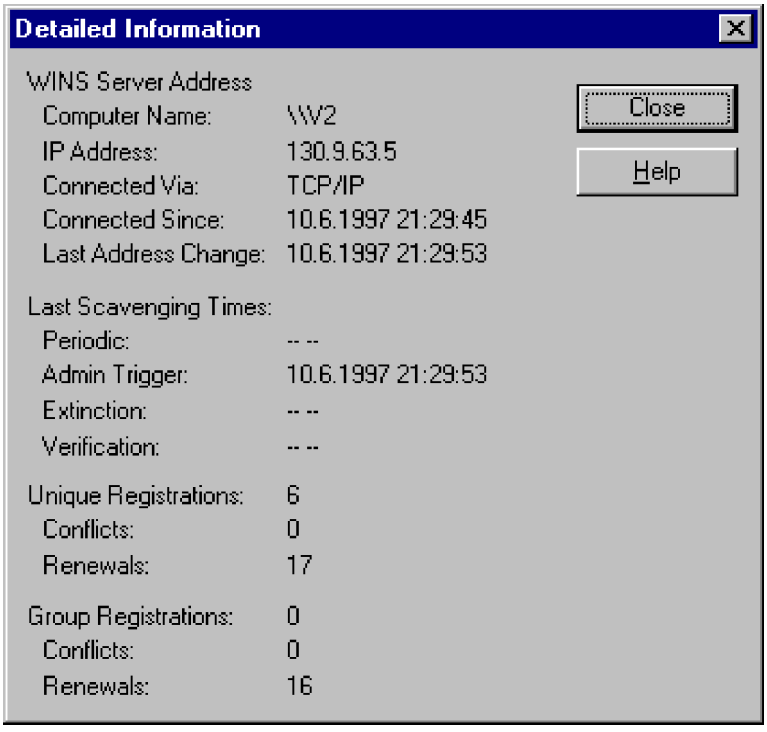
WINS-palvelimen hallinta

Halutun palvelimen voit valita kohteeksi valinnalla **Add | WINS Server**. Anna palvelimen NetBIOS-nimi tai IP-osoite.

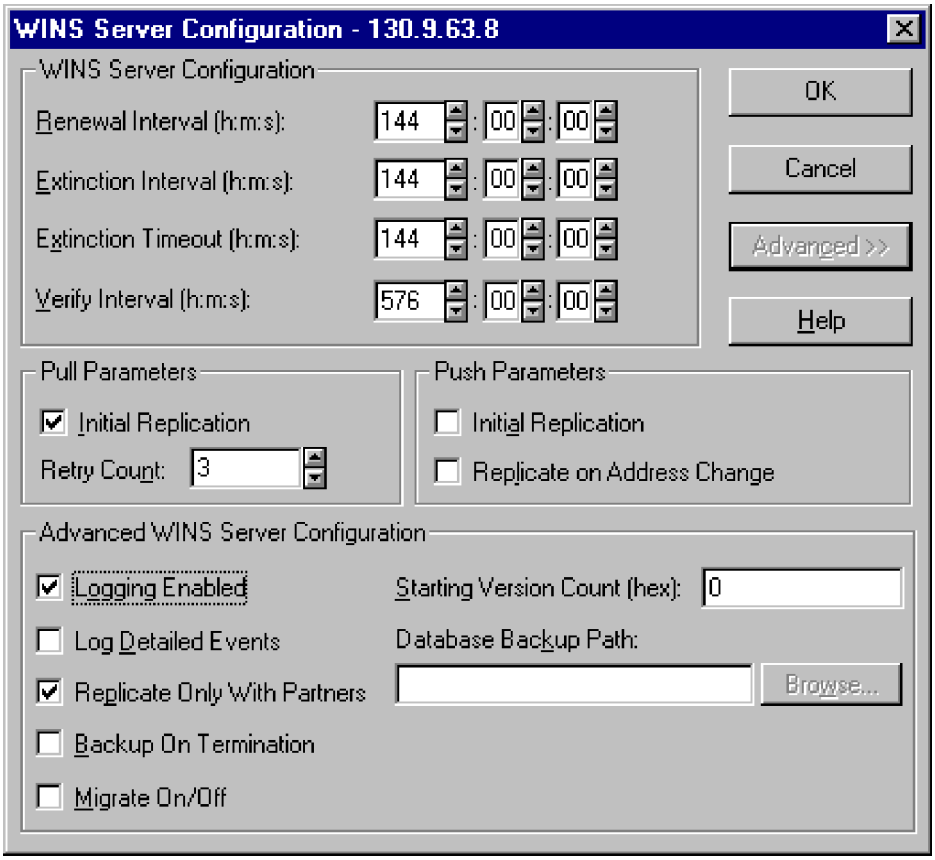
Server-valikolla käsitellään WINS-palvelinta ja WINS-replikointipalvelimia. **View**-valikko tyhjentää tilastot ja **Mappings**-valikosta nähdään nimien ja osoitteiden väliset liitokset. **Options**-valikossa voidaan määritellä lisäasetukset, mm. tilastoinnin ja näytön sekä replikoinnin suhteen.



Valinnalla **Server** | **Detailed Information** näet yhdellä silmäyksellä WINS-palvelimen tilanteen:



WINS:in asetuksia voit muuttaa valinnalla **Server** | **Configuration**.



Asetukset ovat:

- **Renewal Interval, Extinction Interval, Extinction Timeout, Verify Interval** - tietokannan "virkistystaajuus"; asetukset riippuvat toisistaan
- **Pull Parameters, Push Parameters** - tietokannan tietojen vienti- ja tuontiasetukset muille WINS-palvelimille
- **Logging Enabled, Log Detailed Events** - lokin asetukset
- **Replicate Only with Partners** - tietokantaa viedään vain annetuille palvelimille
- **Backup On Termination** - tietokanta varmistetaan, kun WINS-palvelu pysäytetään

- **Migrate On/Off** - käsitelläänkö päällekkäisiä varauksia dynaamisesti

- **Starting Version Count** - kyseisen WINS-tietokannan prioriteetin asetus

- **Database Backup Path** - tietokannan varmistushakemisto.

WINS-palvelinten roolit

WINS-palvelimet voivat välittää toisilleen osoitetietojaan työntö- tai vetomenetelmällä (*Push* / *Pull*). Tällöin puhutaan *Push Partnereista* ja *Pull Partnereista*:

- **Push Partner** lähettää viestin WINS-tietokantansa muuttumisesta Pull Partnereilleen. Kun nämä lähettävät kopiointipyynnön, Push Partner lähettää muuttuneet tiedot Pull Partnereilleen

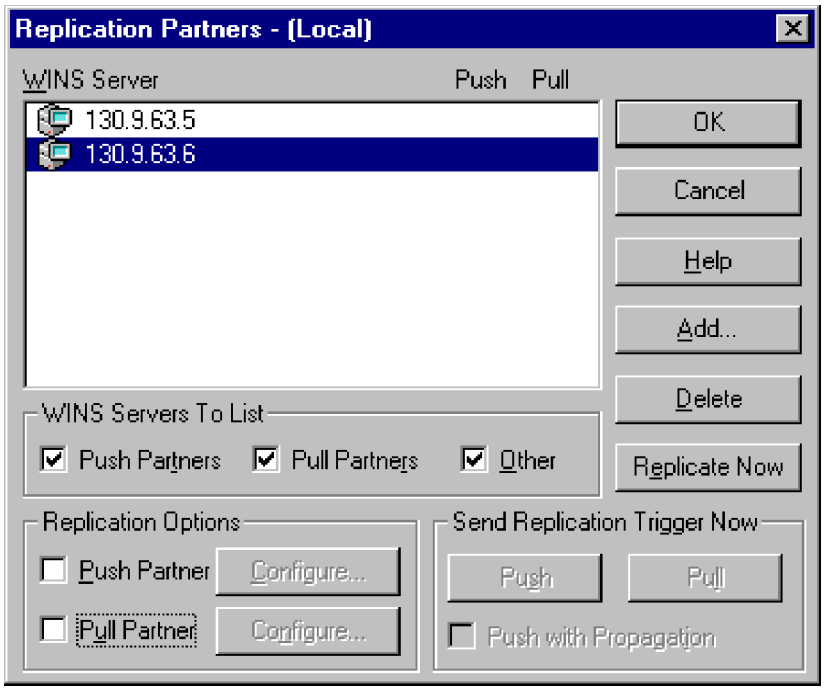
- **Pull Partner** lähettää WINS-tietokannan uusista tiedoista kopiointipyyntöjä Push Partnereilleen. Uudet tiedot erotellaan versionumeroinnin avulla.

Jos haluat **vikasietoisen** WINS-palvelinparin, molemmat voivat olla toistensa Push- ja Pull Partnereita.

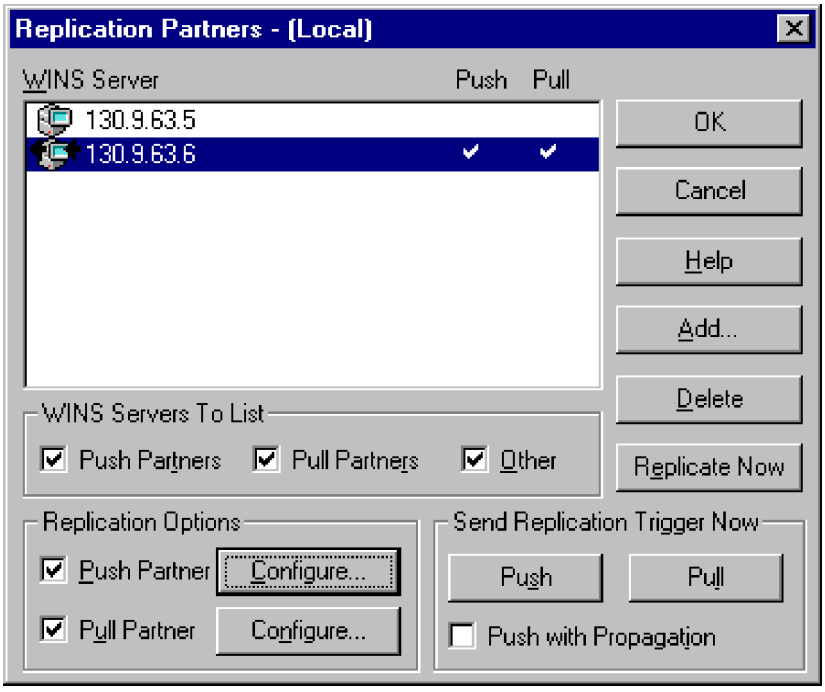
Roolin määrittely tehdään seuraavasti:

1) Valitse **Server** | **Replication Partners**

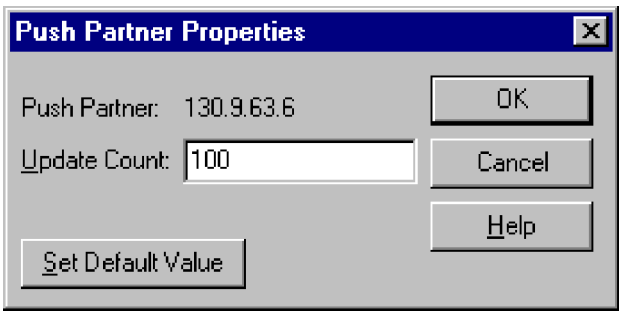
2) Lisää **Add**-painikkeella halutut WINS-palvelimet



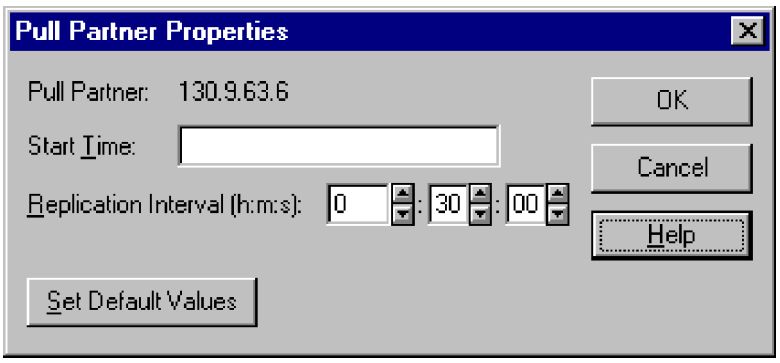
3) Valitse toinen WINS-palvelin ja paina **Replication Options**-kohdan **Push Partner**, **Pull Partner** tai molemmat



4) Paina **Push Partner**-kohdan **Configure**, niin voit määritellä montako uutta tapahtumaa tarvitaan, ennen kuin Push Partner lähettää viestin tietokantansa muuttumisesta

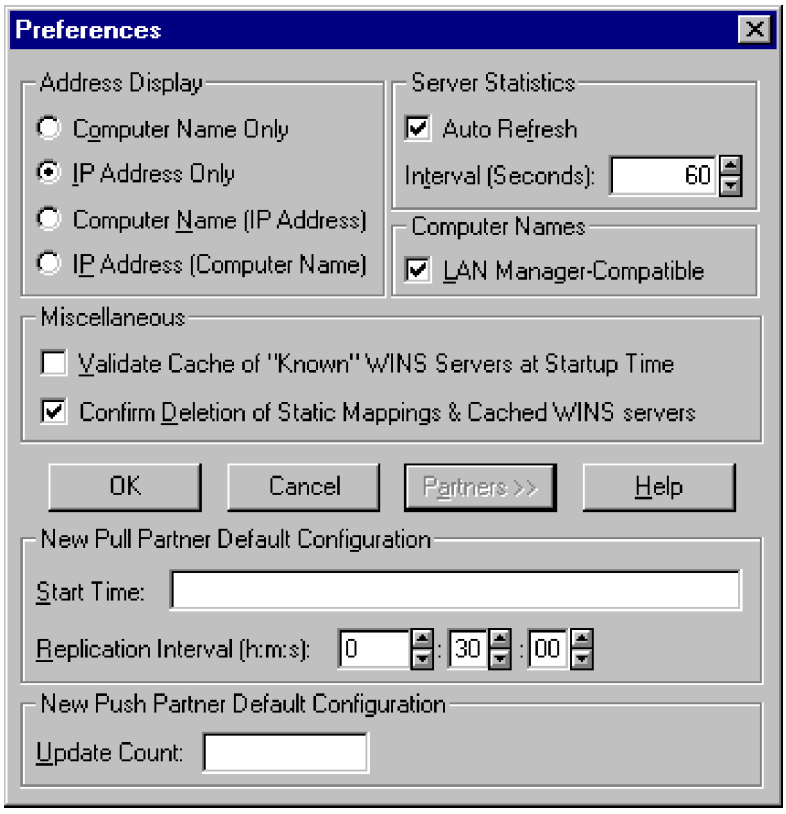


5) Paina **Pull Partner**-kohdan **Configure**, niin voit määritellä useinko Pull Partner lähettää kyselyitä Push Partnerin tietokannan muuttumisesta

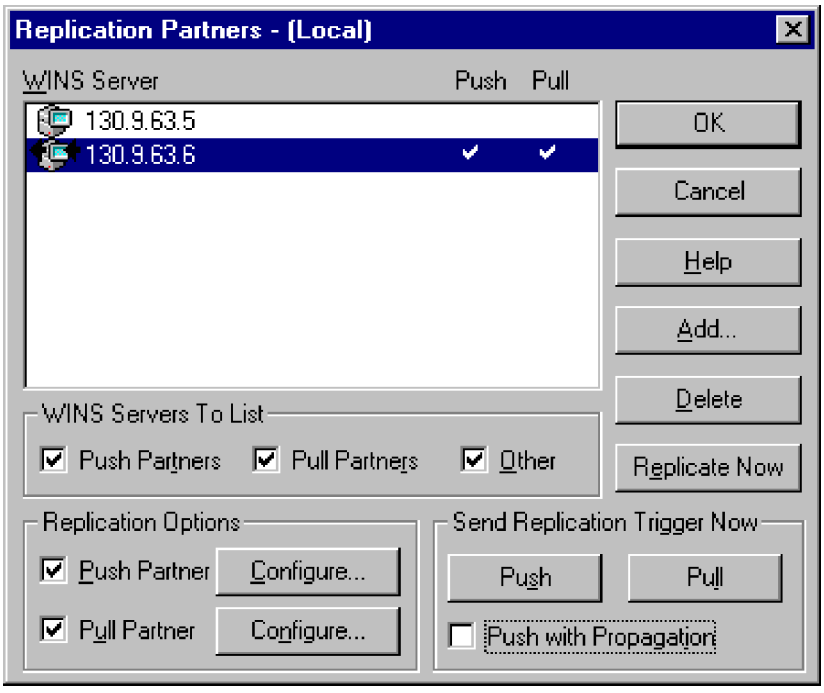


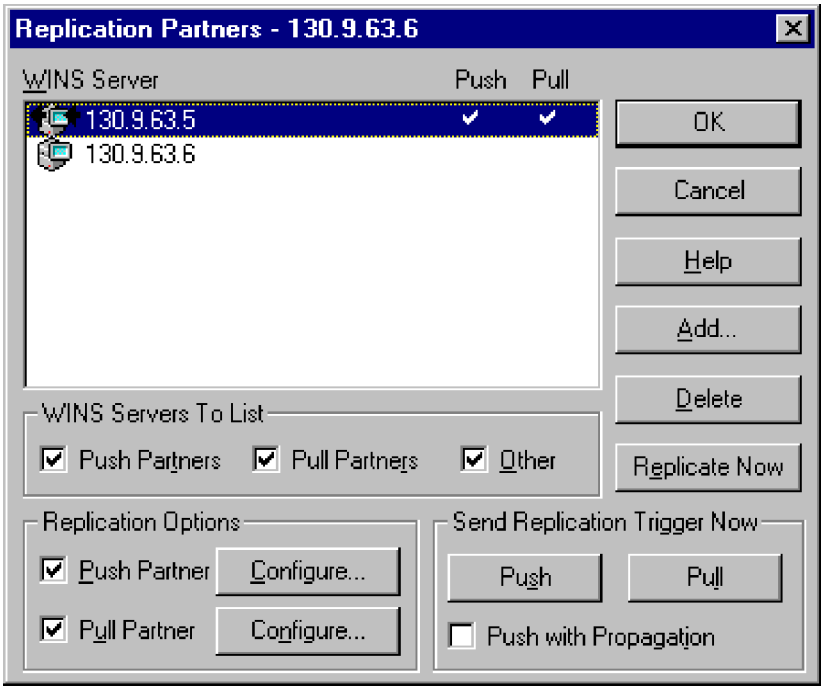
6) Voit tehdä samat operaatiot toisessa WINS-palvelimessakin, niin saat aikaan täydellisen WINS-tietokantojen tapahtumien monistuksen.

Halutut asetukset voidaan määritellä myös valinnalla **Options** | **Preferences**.



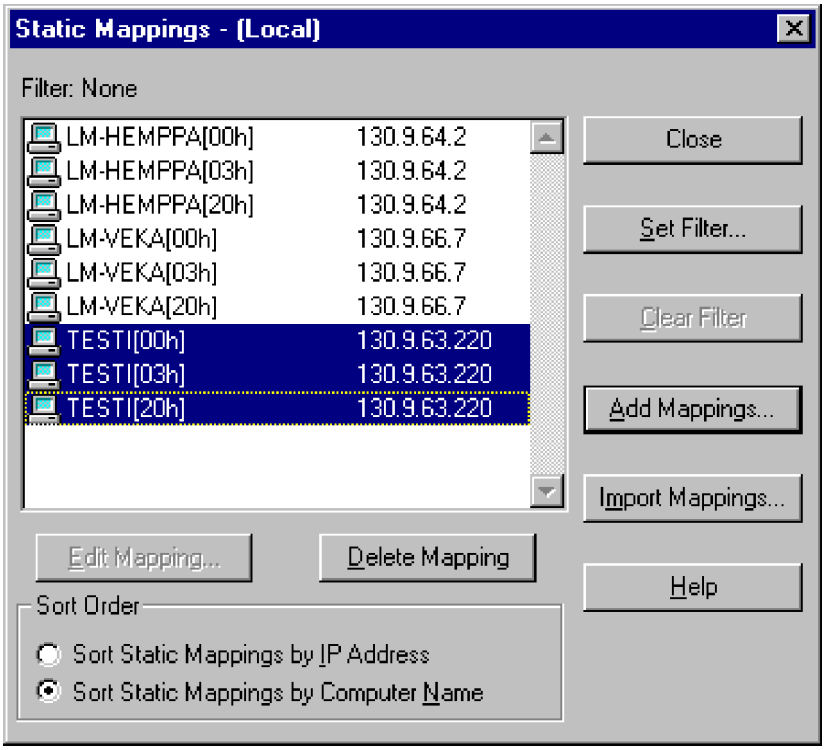
Tässä esimerkissä on kaksi WINS-palvelinta, jotka ovat toistensa Push- ja Pull Partnereita:





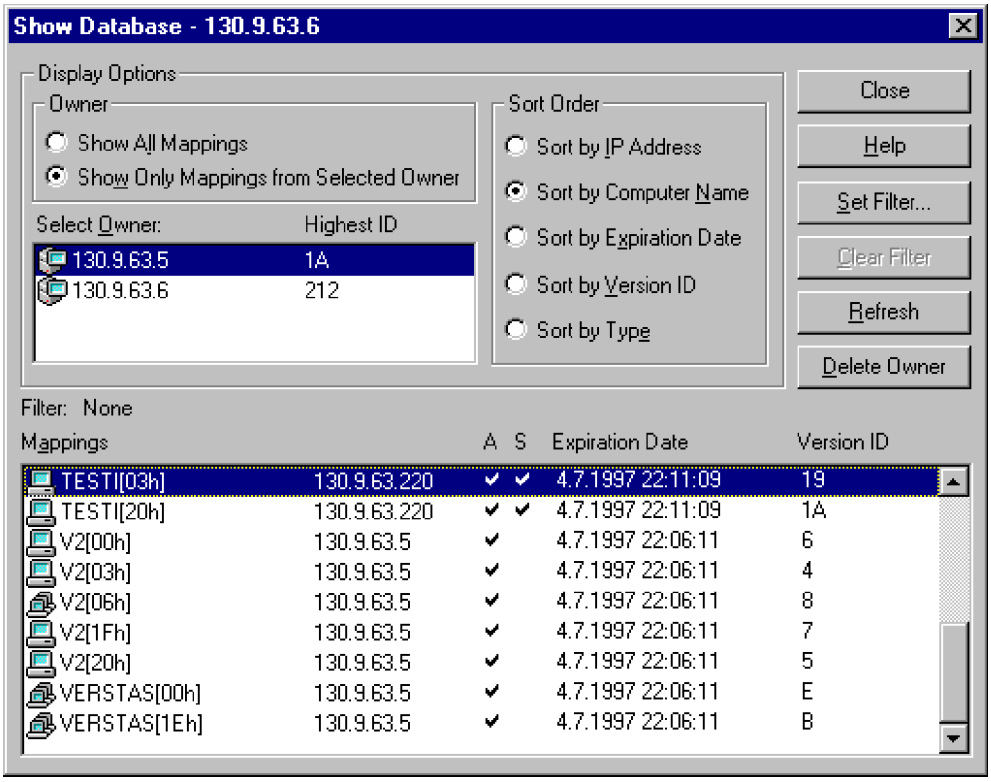
Voit testata toimintaa esimerkiksi luomalla staattisen osoitteen, ja tarkistamalla sen kopioinnin WINS-palvelimelta toiselle seuraavasti:

1) Luo staattinen osoite (tässä esimerkissä luodaan **TESTI**, jonka IP-osoite on **130.9.63.220** WINS-palvelimella **130.9.63.5**)



2) Valitse **Server** | **Replication Partners** ja paina **Replicate Now**

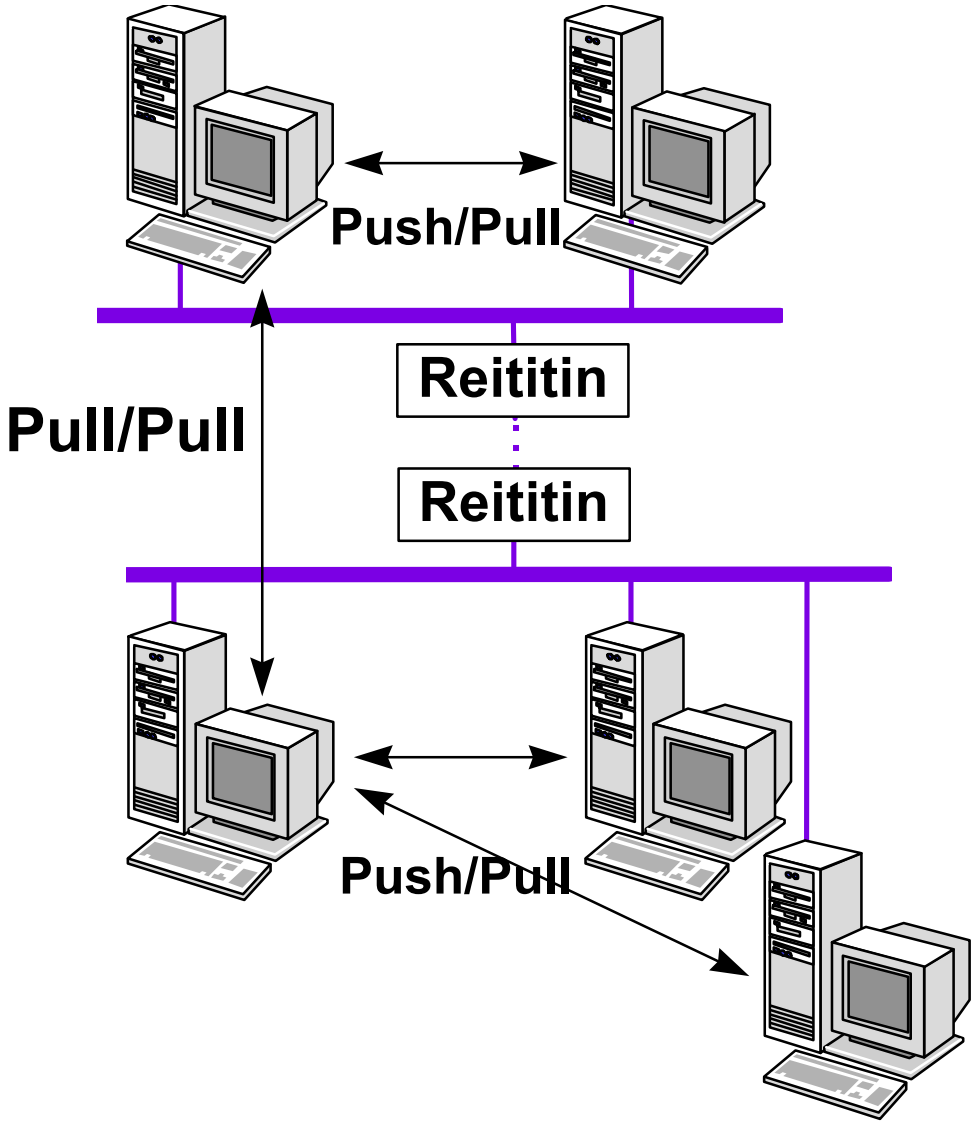
3) Tarkista toisessa palvelimessa **Mappings** | **Show Database** -valinnalla (valitse **Select Owner**-kohdassa edellinen WINS-palvelin) onko nimi kopioitu paikallisen WINS-palvelimen tietokantaan. Tässä esimerkissä näin on:



Periaatteita:

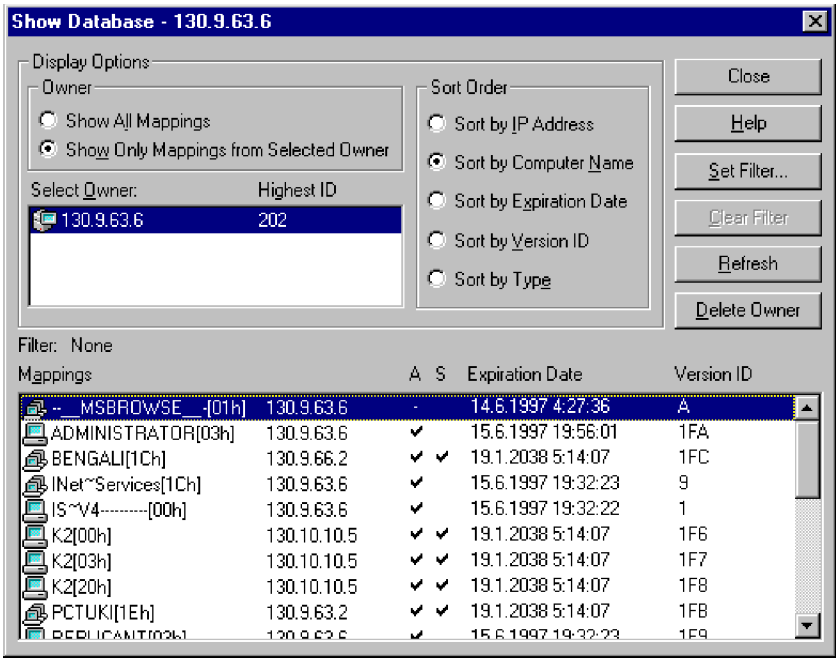
- Määrittele **Pull Partnereita** hitaiden yhteyksien välille, koska Pull Partnerin päivityksiä voidaan säätää
- Määrittele **Push Partnereita** nopeiden yhteyksien välille, koska kopiointi tapahtuu automaattisesti, kun on saavutettu tietty määrä uusia tai päivitettyjäWINS-tietokannan tapahtumia

.


Push/Pull
Reititin
Pull/Pull
Reititin
Push/Pull

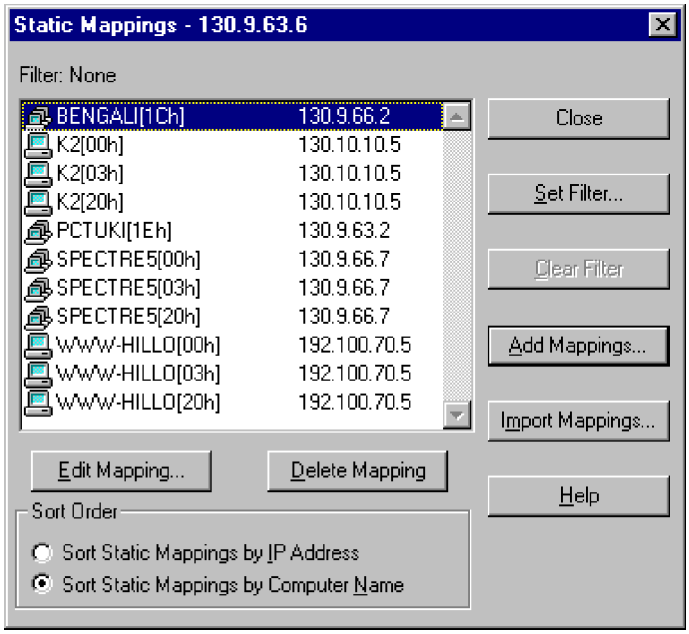
WINS-palvelun käsittelemät nimet

Valinnalla **Mappings | Show Database** nähdään verkossa käytettävät nimet. Kuten huomataan, nimiä voi olla useampiakin samalla osoitteella:



Pysyvät nimien määrittelyt

Valinnalla **Mappings | Static Mappings** voidaan asettaa pysyvästi ja muokata tiettyä NetBIOS-nimeä tietylle osoitteelle.

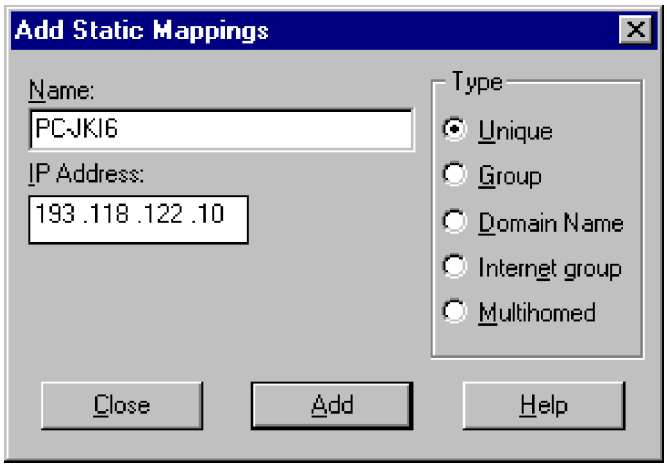


Add Mappings -painikkeella voit lisätä nimen IP-osoitteelle.
Valinnat ovat:

- **Unique** - yksilöllinen, ainutkertainen osoite
- **Group** - ryhmä
- **Domain Name** - toimialueen nimi (1Ch)
- **Internet Group** - käyttäjän määrittelemä ryhmä (20h), max 25 osoitetta
- **Multihomed -** tietokone, jossa on useampi verkkokortti.

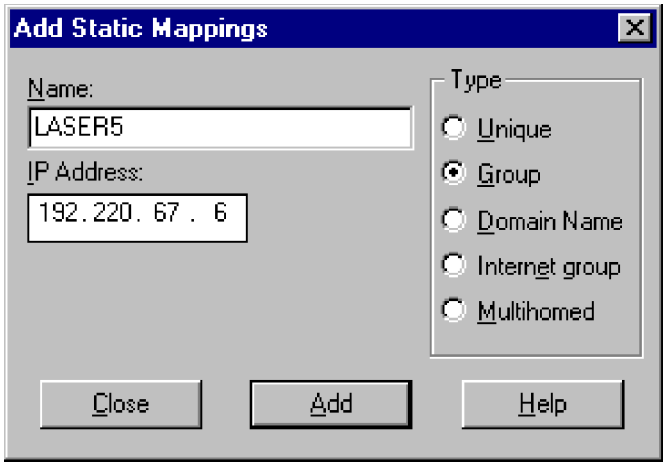
Unique

Unique on yksilöllinen, ainutkertainen osoite - esimerkiksi palvelimen, työaseman tai verkkokirjoittimen osoite. Anna NetBIOS-nimi **Name** -kohtaan ja IP-osoite **IP Address** -kohtaan.



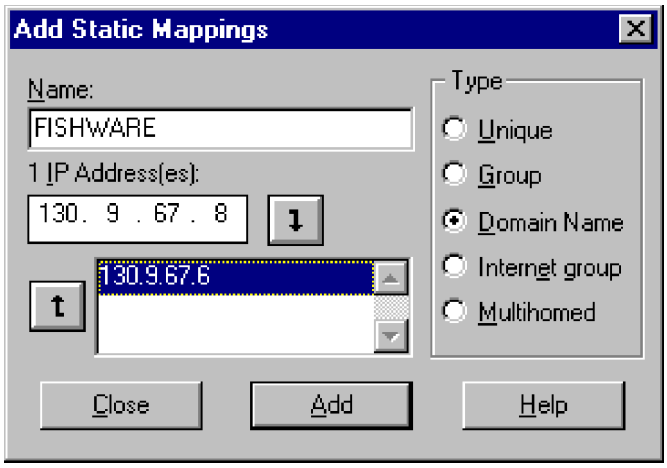
Group

Group on ryhmän nimi. Yleissanomat lähetetään ryhmälle.



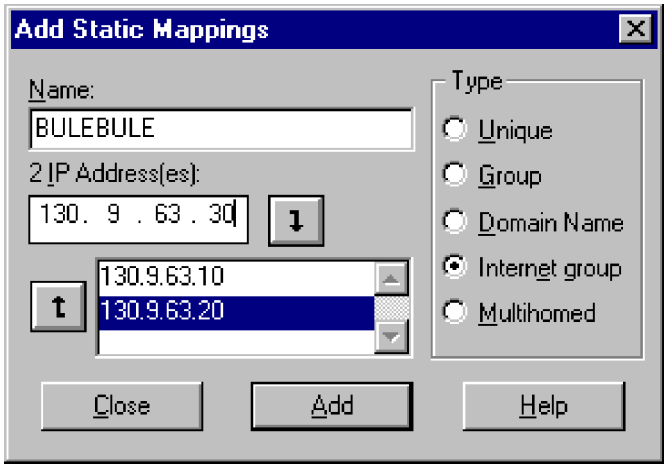
Domain Name

Domain Name on toimialueen nimi. Voit lisätä kaikki toimialueen ohjauskoneet tähän listaan. 25 ohjauskoneen jälkeen WINS kirjoittaa vanhimman määritellyn päälle.



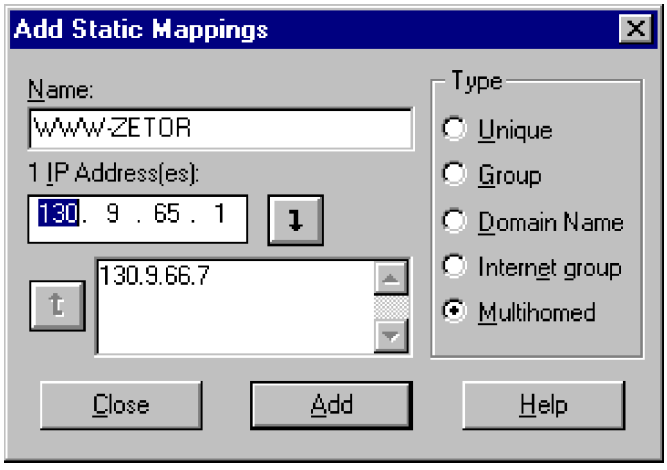
Internet Group

Internet Group on käyttäjän määrittelemä ryhmä (20h), jossa on max 25 osoitetta.



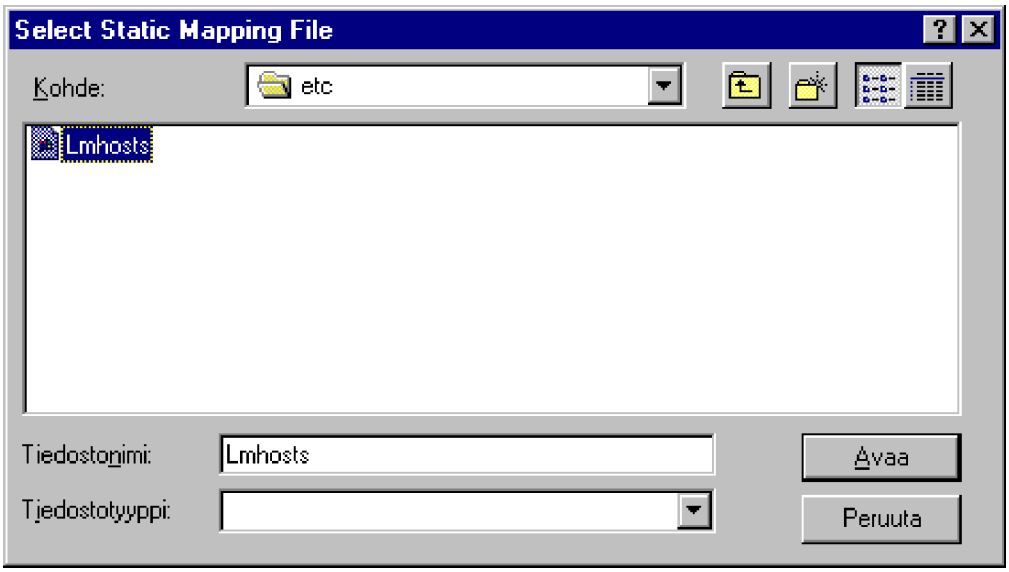
Multihomed

Multihomed on tietokone, jossa on useampi verkkokortti. Määrittele verkkokorttien IP-osoitteet tähän.



Import Mappings

Import Mappings-painikkeella voit tuoda esimerkiksi **LMHOSTS**-tiedoston WINS-palveluun! Tämä tietysti edellyttää, että **LMHOSTS** on tehty aiemmin.



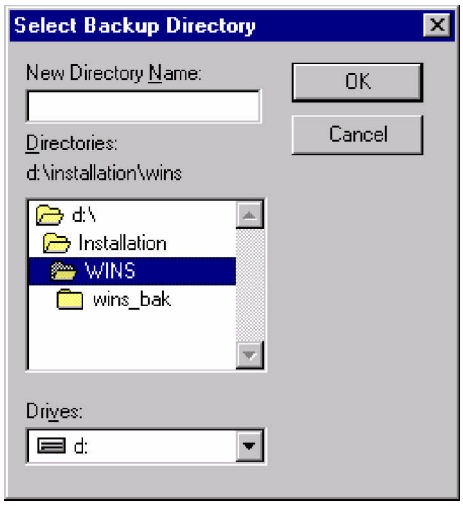
Se löytyy esimerkiksi **Winnt\system32\drivers\etc**-hakemistosta. Jos lisäät LMHOSTS-tiedoston, **Static Mappingsin** tulisi todennäköisesti näyttää erilaiselta aiempaan verrattuna, koska **LMHOSTS**:in staattiset osoite/nimiluettelot on haettu.

WINS-tietokannan varmistaminen

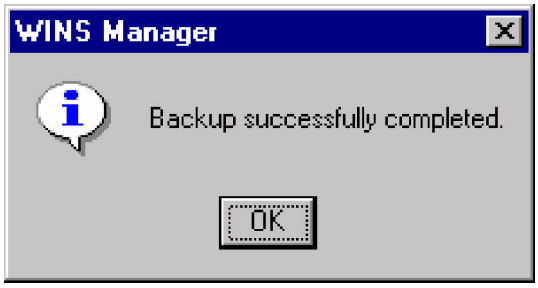
WINS-palvelin käyttää seuraavia tiedostoja **SYSTEM32\DHCP**-hakemistossa:

- **WINS.MDB** - WINS-tietokanta
- **WINSTMP.TMP** - väliaikainen tietokanta WINS:n käytön aikana
- **JET.LOG** - tapahtumatietokanta
- **SYSTEM.MDB** - tietokannan rakennetiedot.

Voit varmistaa WINS-tietokannan valinnalla **Mappings | Backup Database**:



Valitse hakemisto ja paina **OK**: saat ilmoituksen onnistuneesta varmistuksesta.



WINS-tietokannan tiivistäminen

WINS-tietokanta on syytä tiivistää, jos sen koko ylittää 30 Mt. Tilaa vievät:

- Unique / Group -tietue: 50 - 70 tavua
- Internet Group / Multihomed -tietue: 50 - 300 tavua
- Tietuetta kohti on lisäksi 50 - 100 tavun ylimääräinen tilanvaraus.

Tiivistys tehdään seuraavasti:

1) Anna komento **NET STOP WINS**

2) Siirry NT:n järjestelmähakemiston WINS-alihakemistoon (WINNT\System32\WINS) ja anna komento:

JETPACK WINS.MDB WINSTEMP.MDB

3) Tietokanta tiivistetään **WINSTEMP.MDB**-tiedostoon, tiedosto kopioidaan nimelle **WINS.MDB** ja väliaikaistiedosto poistetaan (väliaikaistiedoston nimi voi olla mikä tahansa)

4) Anna komento **NET START WINS**.

Domain Name System

Sekä DNS etä WINS ovat nimiselvitysmenetelmiä. Niiden erot ovat seuraavat:

- **DNS** (Domain Name System) on hierarkinen hajautettu tietokantajärjestelmä **FDQN-nimien** rekisteröintiin ja kyselyihin sekä staattiseen nimien muuntamiseen IP-osoitteiksi. Sen tarkoitus on erilaisten verkkoresurssien nimien muuntaminen IP-osoitteiksi. DNS-palvelinta kutsutaan nimipalvelimeksi.

- **DNS** käyttää staattisia tiedostoja nimenselvitykseen, eikä se tue dynaamista nimi-osoitevastaavuuksien päivittämistä. DNS vaatii IP-osoitteiden staattisen konfiguroinnin, jotta muunnoksia pystyttäisiin tekemään

- **WINS** puolestaan on hajautettu tietokanta **NetBIOS-nimien** rekisteröintiä ja kyselyitä varten. Sen avulla voidaan dynaamisesti muuntaa NetBIOS-nimiä IP-osoitteiksi. WINS taas tukee IP-osoitteiden varaamista DHCP:n avulla ja pystyy näin dynaamisesti muuntamaan NetBIOS-nimiä IP-osoitteiksi.

DNS-nimi on samankaltainen kuin NetBIOS-nimi siinä mielessä, että molemmat ovat käyttäjäystävällisiä (*Friendly name*) nimiä tietokoneelle tai muulle verkkolaitteelle. DNS-nimet muodostavat kuitenkin **hierarkkisen nimiavaruuden**, kun taas NetBIOS-nimet ovat **yksiulotteisia**. DNS-nimi muodostuu kahdesta osasta: **koneen nimestä** (*host name*) ja **palvelinalueen nimestä** (*domain name*). Yhdessä näistä muodostuu **täydellinen koneennimi** (*Fully Qualified Domain Name*, FQDN).

NetBIOS-nimet muistuttavat DNS-nimiä, mutta DNS-nimet voivat olla huomattavasti pidempiä: NetBIOS-nimen maksimipituus on 15 merkkiä ja DNS-nimen 255 merkkiä.

Windows NT:ssä koneen DNS-oletusnimi on sama kuin koneen NetBIOS-nimi. NT muodostaa täydellisen DNS-nimen lisäämällä DNS-palvelinalueen nimen pisteellä erotettuna koneen NetBIOS-nimeen, kuitenkin niin, että NetBIOS-nimen kuudestoista merkki (resurssityypin tunniste) jätetään pois. DNS-oletusnimen muuttamien onnistuu TCP/IP-asetusten DNS-välilehdellä.

Windows NT 4.0:ssa on myös mahdollista muodostaa NetBIOS over TCP/IP (NetBT)-yhteys käyttämällä IP-osoitetta, FQDN-nimeä tai NetBIOS-nimeä.

DNS-nimipalvelu

Windows NT Server 4.0:aan kuuluu RFC-yhteensopiva nimipalvelu (Domain Name System, DNS). DNS on määritelty RFC:issä 1034 ja 1035. Tietoja DNS:n tekniikasta löytyy Albitz & Liun **DNS and BIND**-kirjasta, kustantaja **O Reilly and Associates** (ISBN 1-56592-010-4).

DNS on globaali, hajautettu tietokanta, joka perustuu hierarkkiseen nimikäytäntöön. Nimeämiskäytäntö kehitettiin alunperin, jotta verkossa olevat tietokoneet ja muut laitteet pystyttäisiin yksilöllisesti tunnistamaan internetissä ja muissa TCP/IP-verkoissa. DNS-tietokannan juuritietoja ylläpitää **Internet Network Information Center**. Ylimmän tason alueita ovat organisaatio- ja maatunnukset.

DNS-nimi koostuu kahdesta osasta, alueen nimestä ja tietokoneen nimestä. Yhdessä nämä muodostavat **täydellisen koneennimen** (*Fully Qualified Domain Name*, FQDN).

Esimerkiksi FishWare Oy -yrityksen mikrotukihenkilön työasema voisi olla nimeltään **orja5.tietohallinto.fishware.fi**. Tässä itse työaseman nimi on **orja5**. Nimi voi siis muodostua useista osista, jotka erotetaan toisistaan pisteellä.

DNS käyttää asiakas/palvelin-mallia. Yksi DNS-nimipalvelin sisältää tiedot jostakin DNS-nimiavaruuden osasta, vaikkapa organisaation sisäisestä intranetistä. DNS:n käyttäjä (asiakastietokone) pyytää DNS-palvelimelta nimeä vastaavaa IP-osoitetta. Nimenselvitystoiminnot on usein rakennettu sisään asiakassovellukseen tai ne ovat asiakaskoneella ohjelmakirjastona kaikkien ohjelmien käytettävissä.

Nimipalvelu on lähtöisin **ARPANET**:ista, jossa nimenselvitys alkujaan hoidettiin yksinkertaisella tekstitiedostolla nimeltä **HOSTS**. Kun tietokoneiden määrä oli pieni, **HOSTS**-tiedoston ylläpitäminen oli helppoa. Tiedostossa oli yksinkertaisesti lueteltu koneen nimet ja niitä vastaavat IP-osoitteet pareittain. Yhteinen HOSTS-tiedosto siirrettiin aika ajoin kaikkiin ARPANET-verkkoihin, ja nimenselvitys hoidettiin paikallisesti sen avulla. Kun ARPANET kuitenkin kasvoi ja muuttui

internetiksi, verkossa olevien tietokoneiden määrä kasvoi räjähdysmäisesti ja koko verkon kattava nimenselvitys yhden tekstitiedoston avulla kävi mahdottomaksi.

Tarvittiin uusi ratkaisu, ja se oli hajautettu, hierarkinen nimiavaruus, jonka ylläpito olisi mahdollisimman helppoa. Tavoitteena DNS:n alkuperäisten kehittäjien mukaan oli seuraava:

- Korvata kömpelö, keskitetysti hoidettu HOSTS-tiedosto kevyellä, hajautetulla tietokannalla, jonka nimiavaruus olisi hierarkinen
- Joka mahdollistaisi hajautetun ylläpidon ja laajennettavat datatyypit
- Voisi kasvaa liki rajattomasti ja olisi silti kohtuullisen suorituskykyinen.

DNS on OSI-mallin tasolla seitsemän ja voi käyttää protokollanaan sekä **UDP**:tä että **TCP**:tä (molemmissa porttia **53**). Aluksi asiakkaat lähettävät nimiselvityspyynnön palvelimelle tehokkaammalla **UDP**-protokollalla ja siirtyvät yhteydelliseen **TCP**:hen vain, jos palautettu data näyttää virheelliseltä. Palvelimet käyttävät TCP:tä nimitietojen vaihtamiseen.

Suosituin DNS-toteutus on **BIND** (*Berkeley Internet Name Domain*), alun perin **BSD Unix 4.3**:lle kehitetty palvelu (DNS-määritykset löytyvät RFC-dokumenteista 974, 1034 ja 1035)

DNS:ssä on kolme pääkomponenttia (RFC 1034):

- **Nimiavaruus ja resurssitietueet** - nimiavaruus on strukturoitu kokonaisuus, joka muistuttaa ylösalaisin käännettyä puuta. Puun oksat ja lehdet vastaavat jotakin informaatiokokonaisuutta. Resurssitietueet (*Resource records*) ovat tietueita, joiden avulla DNS:ää voidaan konfiguroida (esimerkiksi **SOA**-tietue (*Start of Authority*)), tai tietueita jotka sisältävät erityyppistä informaatiota kyselyiden ratkaisemiseksi (esimerkiksi **A** (*Address*) ja **MX** (*Mail Exchanger*)). Yleensä resurssitietueissa on verkkoresursseja ja niitä vastaavia IP-osoitteita. Kyselyoperaatiossa etsitään tietoja tietyn tyyppisistä resurssitietueista. Tällöin pitää syötteenä määritellä nimi sekä pyydettävä tietotyyppi. Esimerkkikyselyssä saatettaisiin palvelimelle kertoa tietokoneen nimi ja pyytää sitä vastaava IP-osoite.

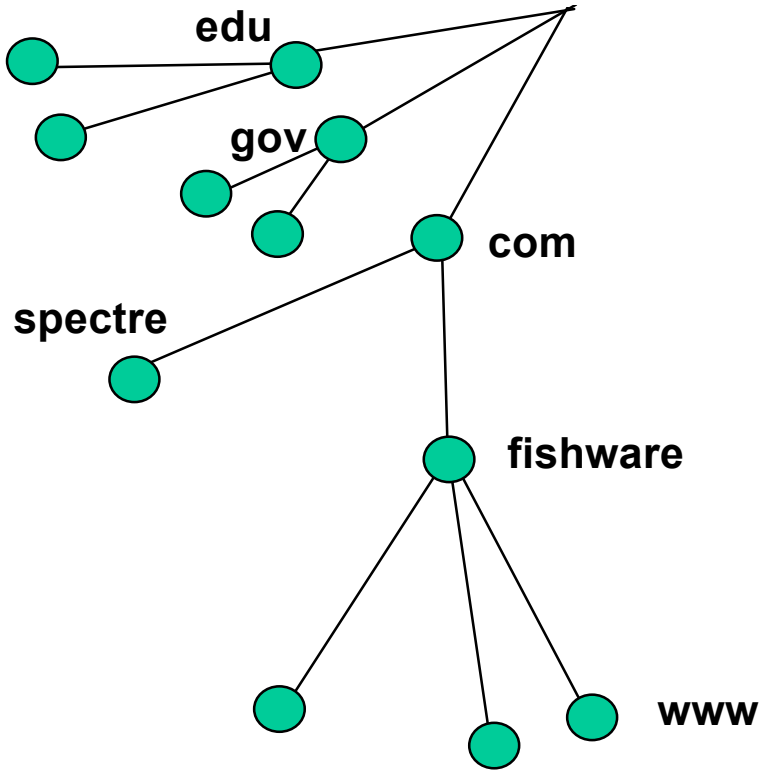
- **Nimipalvelimella** ajetaan ohjelmistoa, joka huolehtii resurssitietueiden ylläpidosta ja yrittää selvittää nimikyselyitä. Yleensä nimipalvelin joko löytää vastauksen omista tietueistaan tai osaa välittää kyselyn jollekin toiselle nimipalvelimelle, joka pystyy auttamaan nimiselvityksessä. Jos nimipalvelimella on tietyn verkkoalueen nimitiedot, sitä kutsutaan kyseisen nimiavaruuden osan **auktoriteetiksi**, jonka alainen informaatio on jaettu vyöhykkeisiin (*Zone*).

- **Selvittäjät** (*Resolver*) lähettävät pyyntöjä nimipalvelimelle asiakasohjelman puolesta. Yleensä selvitysrutiinit on rakennettu sisään sovellusohjelmiin tai ne ovat käytettävissä erillisinä kirjastoina.

Verkkoalueet ja niiden osat

DNS-nimiavaruus on looginen puurakenne. Jokaisella haaralla tässä puussa on enintään 63 merkin pituinen nimi. Puun juurella on erityisnimi (*null*). Jokainen haara on nimiavaruuden osa, jota kutsutaan verkkoalueeksi (*domain*). Verkkoalue voi esiintyä missä tahansa puun kohdassa. Kukin verkkoalue voi edelleen jakautua uusiksi verkkoalueiksi ylläpidon helpottamiseksi tai kuormituksen vähentämiseksi. Verkkoalueen nimi (*domain name*) kertoo alueen sijainnin puurakenteen sisällä. Täydellinen verkkoaluenimi (*Full domain name*) puolestaan kertoo sijainnin suhteessa juureen.

Verkkoaluenimi muodostetaan liittämällä kunkin haaran nimet peräkkäin pisteellä erotettuna, lähimmästä haarasta aina juureen asti. Verkkoalueita voidaan ryhmitellä vyöhykkeiksi, jotta hajautettu ylläpito olisi mahdollista.



Jos haluttaisiin ottaa yhteys alueen **FISHWARE.COM** sisällä olevaan koneeseen **WWW**, pitäisi antaa täydellinen verkkoaluenimi (*Fully Qualified Domain Name*, FQDN) **WWW.FISHWARE.COM**. Alue **FISHWARE.COM** kuuluu ylimmän tason **COM**-alueen alaisuuteen.

Ylimmän tason verkkoalueita ylläpitää **InterNIC** (*Internet Network Information Center*). Alemman tason verkkoalueita ylläpitää alueesta vastaava organisaatio, esimerkiksi **FISHWARE.COM**-alueen tapauksessa **Fishware**-yhtiö. Kuvassa on myös **SPECTRE.COM**.

DNS ja internet

Verkkoalueet ovat hierarkkisen järjestelmän eri tasoja. Hierarkian huippua kutsutaan juureksi, ja juurialueella ei ole nimeä. Siihen voidaan kuitenkin tarvittaessa viitata käyttämällä pistettä (.).

Nimijärjestelmä on lähtöisin Yhdysvalloista, ja siellä juuritasolla on seitsemän InterNICin ylläpitämää nimipalvelinta. Juuritason alla ovat niin sanotut ylimmän tason verkkoalueet, jotka on jaettu alueen luonteen mukaan sekä maakohtaisesti. Nämä alueet ovat:

DNS-toimialueen lyhenne	Organisaatio	Esimerkki
com	Commercial, kaupallinen sektori	**nokia.com**
edu	Educational, koulutussektori	**mit.edu**
gov	Government, julkinen sektori	**nsf.gov**
org	Organizations, ei-kaupallinen sektori	**w3.org**
mil	Military, USA:n sotilasverkko	**pentagon.mil**
net	Networking, verkko-organisaatiot	**nsf.net**
int	International, kansainväliset organisaatiot	**redcross.int**
xx	valtakunnalliset, kaksikirjaiminen maakoodi	**fi**

Kullakin ylimmän tason verkkoalueella on InterNICin ylläpitämä nimipalvelin. Näiden verkkoalueiden sisällä voi olla toisia verkkoalueita sekä koneita.

Koneennimet

Koneennimi liitetään verkkoaluenimen alkuun pisteellä erotettuna. Useimmiten koneesta puhutaan sen täydellisellä nimellä, eli nimellä jossa on mukana koko verkkoaluenimi. Esimerkiksi palvelin nimeltä **WWW** verkkoalueella **RUBBERDUCK.COM** olisi koko nimeltään **WWW.RUBBERDUCK.COM**.

Koneen nimen antaa yleensä ylläpitäjä, jotta TCP/IP-verkossa oleva laite olisi helpompi tunnistaa. Microsoft-verkoissa nimen ei tarvitse olla sama kuin tietokoneen nimi (**Computername**), mutta se voi helpottaa verkon ylläpitoa. Nimessä voi olla 256 merkkiä.

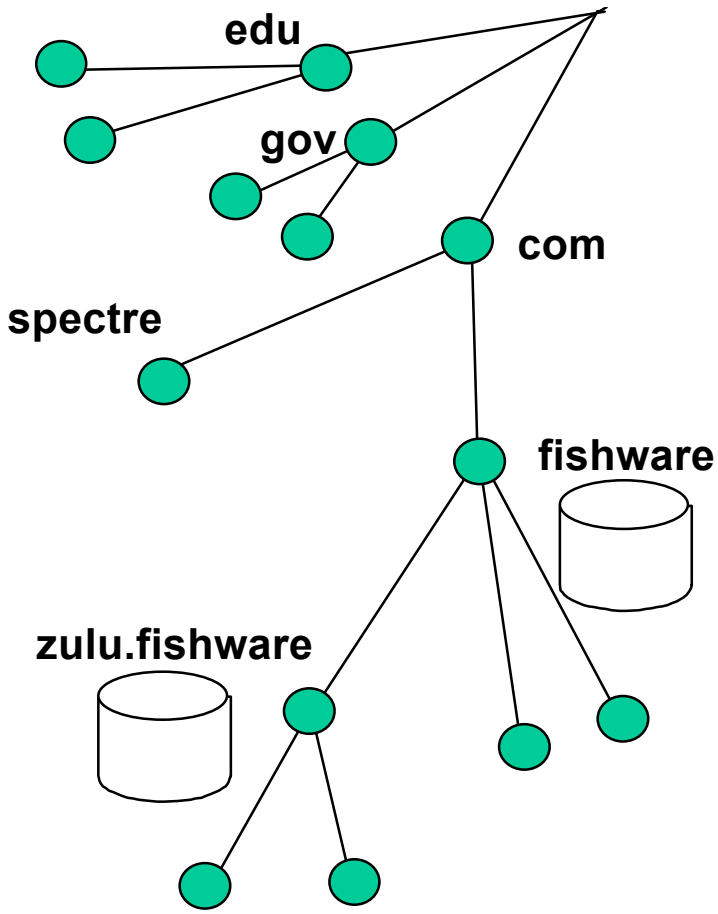
Samaan IP-osoitteeseen voi liittyä useitakin nimiä joko **HOSTS**-tiedostossa tai **DNS**-palvelussa, vaikka Windows NT:n Ohjauspaneelin kautta onkin mahdollista määritellä vain yksi nimi. Nimet ovat helpompia muistaa kuin numeeriset IP-osoitteet, ja niitä voidaan käyttää IP-osoitteen sijasta erilaisia verkko-ohjelmia käytettäessä.

HOSTNAME-ohjelma näyttää käyttämäsi koneen IP-osoitetta vastaavan nimen. Oletusarvoisesti se on Windows NT- ja Windows 95 -koneilla sama kuin tietokoneen nimi (**Computername**).

Vyöhykkeet

Vyöhyke on DNS-nimiavaruuden osa, jonka tietueet ovat tietyssä vyöhyketiedostossa. Yksittäisellä DNS-palvelimella voi olla yksi tai useampi vyöhyketiedostoja. Jokainen vyöhyke kiinnittyy tiettyyn verkkoalueen haaraan, jota kutsutaan vyöhykkeen juurialueeksi (*Root domain*). Vyöhyketiedostossa ei välttämättä ole kaikkia saman, juurialueen alaisen haaran nimitietoja eli joidenkin alihaarojen tiedot voivat puuttua.

Verkkoalue saattaa esimerkiksi jakaantua useisiin alueisiin, joista kullakin on oma DNS-palvelimensa. Näiden verkkoalueiden jakaminen useisiin vyöhyketiedostoihin saattaa olla tarpeen, jotta ylläpito voitaisiin hoitaa tarpeeksi hajautetusti tai tietojen monistaminen olisi tehokasta.
Kuvan esimerkissä on verkkoalue **FISHWARE.COM**, mutta koko alueen nimitiedot eivät ole samassa vyöhyketiedostossa. Osa on vyöhykkeessä **FISHWARE.COM** ja osa vyöhykkeessä **ZULU.FISHWARE.COM**. Kummankin vyöhykkeen juurialue on **FISHWARE.COM**.



Nimipalvelimet

DNS-palvelimet varastoivat informaatiota verkkoalueen nimiavaruuden eri osista. Kun DNS-palvelin on vastuussa yhdestä tai useammasta vyöhykkeestä, sitä kutsutaan kyseisten vyöhykkeiden **valtuutetuksi palvelimeksi** (*Authoritative server*). Edellisen esimerkin mukaan nimipalvelin, joka huolehtii vyöhykkeestä **ZULU.FISHWARE.COM**, on kyseisen vyöhykkeen **valtuutettu** palvelin.

Kun DNS-palvelin konfiguroidaan, sille kerrotaan nimipalvelintietueilla (NS- eli *name server* -tietueet), mitä muita nimipalvelimia samaan verkkoalueeseen kuuluu. Jos siis edellisen esimerkin kaksi vyöhykettä olisivat eri nimipalvelimilla, niille pitäisi kertoa toistensa olemassaolosta NS-tietueella.

Nimipalvelimia on useita erilaisia, ja tyyppi riippuu tehtävästä:

- **Ensisijainen nimipalvelin** (*Primary*) saa tietonsa paikallisesti ylläpidetyistä tiedostoista. Muutokset vyöhykkeeseen, kuten verkkoalueiden tai tietokoneiden lisääminen, tehdään ensisijaiseen nimipalvelimeen

- **Toissijainen** (*Secondary*) nimipalvelin saa vyöhyketietonsa monistamalla ne toiselta palvelimelta (joko ensi- tai toissijaiselta). Vyöhyketietojen monistamista kutsutaan **vyöhykesiirroksi** (*zone transfer*). Vyöhykesiirto käyttää TCP-porttia **53**.

Seuraavien syiden vuoksi organisaatiossa kannattaa käyttää toissijaista nimipalvelinta:

- **Vikasietoisuus** - ainakin yksi ensisijainen ja yksi toissijainen nimipalvelin jokaista vyöhykettä kohti on tarpeen virhetilanteiden varalta

- **Etäyhteydet** - paikallista nimipalvelinta tarvitaan, kun etäyhteyden (esimerkiksi RAS) päässä on suuri joukko asiakaskoneita. Etäasiakkaiden ei pitäisi joutua tekemään DNS-kyselyjä hitaiden yhteyksien yli

- Ensisijaisen nimipalvelimen **kuormituksen vähentäminen**.

Koska joka vyöhykkeen informaatio on tallennettuna erilliseen tiedostoon, jako ensi- ja toissijaisiin palvelimiin tapahtuu vyöhyketasolla; toisin sanoen jokin palvelin saattaa olla samalla yhden vyöhykkeen ensisijainen (*Primary*) ja toisen vyöhykkeen toissijainen (*Secondary*) palvelin.

Kun toissijaiselle nimipalvelimelle määritellään vyöhykettä, tämä tehdään sen nimipalvelimen avulla, josta vyöhyketiedot noudetaan. Tätä palvelinta kutsutaan päänimipalvelimeksi (*Master Name Server*), ja se voi olla joko ensi- tai toissijainen nimipalvelin kyseisellä vyöhykkeellä. Kun toissijainen nimipalvelin käynnistyy, se ottaa yhteyden päänimipalvelimeen ja aloittaa vyöhykesiirron kaikkien niiden vyöhykkeiden tiedoille, joissa se on toissijaisena nimipalvelimena.

Vyöhykesiirrot voidaan myös konfiguroida tapahtumaan säännöllisin väliajoin, mikäli johtavalla nimipalvelimella olevat tiedot ovat muuttuneet. Tämä aikaväli määritellään **SOA**-tietueessa (*Start of Authority*).

Kun DNS-palvelin vastaanottaa kyselyn, se yrittää etsiä vastauksen omista vyöhyketiedostoistaan. Jos mitään ei löydy, siitä syystä että palvelin ei ole kyseisen vyöhykkeen valtuutettu palvelin (*Authoritative server*), eikä sillä ole pyydettyä tietoa välimuistissa, nimipalvelimen täytyy käyttää muita nimipalvelimia.

Jos kyseessä on suuri verkko, kuten internet, DNS-kysely oman vyöhykkeen ulkopuolelle vaatii WAN-yhteyden organisaation ulkopuolelle. Tällöin tarvitaan ulkopuolisten kyselyiden tekoon tarkoitettu palvelin, mitä varten DNS:ssä käytetään välittäjiä (*Forwarder*). Tietyt DNS-palvelimet asetetaan toimimaan välittäjinä, ja **vain** nämä nimipalvelimet ottavat yhteyksiä oman verkon ulkopuolelle.

Muut nimipalvelimet käyttävät välittäjiä kahdella menetelmällä hyväkseen:

- Nimipalvelin ottaa yhteyden välittäjään vasta silloin, jos sen **omista tiedoista ei löydy vastausta** kyselyyn. Tällöin välittäjä ottaa yhteyden ulkopuolelle ja palauttaa kysyvälle palvelimelle lopputuloksen. Jos välittäjä ei löydä vastausta, kysyvä palvelin yrittää ratkaista pyynnön itse.

- Nimipalvelin ei yritäkään ratkaista pyyntöä itse, vaan **toimittaa sen suoraan** välittäjälle. Jos välittäjä ei löydä vastausta, nimipalvelin palauttaa asiakkaalle virheen. Tällaista nimipalvelinta kutsutaan orjaksi (*Slave*).

Jos organisaatio on yhteydessä internettiin, omaa DNS-palvelinta ylläpitoineen ei välttämättä tarvita lainkaan. Pienissä verkoissa on todennäköisesti edullisempaa käyttää internet-palveluiden tarjoajan DNS-palvelua. Palveluntarjoajat saattavat periä DNS-ylläpidosta maksun, joten kannattaa verrata eri vaihtoehtojen kustannuksia. Organisaation verkkoaluenimi ja vähintään kaksi DNS-palvelinta täytyy kuitenkin rekisteröidä. Tämä ei tietenkään koske pelkästään sisäisessä käytössä olevia DNS-palvelimia.

DNS-palvelimina tulisi käyttää vähintään kahta konetta, jotta järjestelmä olisi luotettava. Ensisijainen nimipalvelin ylläpitää tällöin tietoja, jotka monistetaan toissijaiselle palvelimelle. Tällä tavoin nimipalvelu toimii,

vaikka toinen palvelimista olisikin poissa käytöstä. Monistusväli riippuu siitä, kuinka usein palvelinnimet muuttuvat. Sen tulisi kuitenkin olla riittävän tiuha, jotta tiedot pysyvät ajan tasalla. Toisaalta hyvin pieni väli voi aiheuttaa kohtuuttomasti verkkoliikennettä ja kuormittaa palvelimia liikaa.

Välimuistipalvelimet

Vaikka kaikki DNS-palvelimet tallentavat kyselyjen tulokset välimuistiin, tämä on ainoa tehtävä **välimuistinimipalvelimilla** (*Caching-only Server*). Ne eivät ole minkään verkkoalueen valtuutettuja palvelimia (*Authoritative server*), eivätkä ne säilytä mitään muita tietoja kuin välimuistiin keräämänsä vastaukset.

Kun välimuistipalvelin käynnistyy, se ei yritä päivittää tietojaan miltään muulta palvelimelta. Palvelimen on siis välitettävä kyselyt eteenpäin, kunnes välimuistiin kertyy tietoja ja se voi etsiä vastauksia suoraan sieltä.

Nimiselvitys

Asiakas voi tehdä DNS-palvelimelle kolmenlaisia kyselyitä: rekursiivisia, iteratiivisia ja käänteisiä. Nimiselvitystä tehtäessä yksi nimipalvelin voi toimia toisen nimipalvelimen asiakkaana:

- **Rekursiivisessa kyselyssä** nimipalvelinta pyydetään vastaamaan joko etsityllä tiedolla tai ilmoituksella siitä, että tietoa ei löytynyt. Palvelin ei voi välittää tietoa edelleen toiselle nimipalvelimelle. Tällaisen pyynnön lähettää yleensä DNS-asiakas (*resolver*) DNS-palvelimelle. Jos palvelin on konfiguroitu käyttämään välittäjää, sen välittäjälle lähettämä kysely on rekursiivinen

- **Iteratiivisessa kyselyssä** kyselyn vastaanottava nimipalvelin antaa parhaan mahdollisen vastauksen, jonka se tietojensa perusteella saa aikaan. Tyypillinen tällainen vastaus on viittaus toiseen nimipalvelimeen, joka luultavasti pystyy vastaamaan alkuperäiseen kyselyyn. Iteratiivisia kyselyitä käytetään nimipalvelinten välillä etsittäessa vastausta asiakkaan rekursiiviseen kyselyyn

- **Käänteinen kysely** tulee kysymykseen, kun asiakas haluaakin tietää jotakin IP-osoitetta vastaavan konenimen. Koska DNS-tietokannassa IP-osoitteen ja koneen nimen välillä ei ole mitään suoraa suhdetta, ainoa varma tapa löytää vastaus olisi käydä läpi kaikki verkkoalueet yksi osoite kerrallaan. Tällaisen tilanteen varalta on luotu erityinen verkkoalue nimeltä **IN-ADDR.ARPA**. Tämän alueen kaikki haarat on nimetty numeeristen IP-osoitteiden mukaan. Koska IP-osoitteet kuitenkin tarkentuvat luettaessa vasemmalta oikealle ja koneennimet luettaessa oikealta vasemmalle, täytyy IP-osoitteen oktetit kääntää päinvastaiseen järjestykseen, kun aluetta **IN-ADDR.ARPA** luodaan. Tällä tavoin alueen **IN-ADDR.ARPA** alempien haarojen ylläpito voidaan sälyttää niille organisaatioille, joille luokkien A, B ja C IP-osoitteita myönnetään.

Kun alue IN-ADDR.ARPA on luotu, käytetään erityisiä **PTR-resurssitietueita** (*Pointer*) kytkemään IP-osoitteet koneennimiin. Jotta osoitetta **130.9.63.5** vastaava nimi löytyisi, asiakkaan täytyy lähettää palvelimelle PTR-tietuetta **5.63.9.130 IN-ADDR.ARPA** koskeva pyyntö. Löytynyt PTR-tietue sisältää osoitetta **130.9.63.5** vastaavan nimen, joka lähetetään takaisin asiakkaalle. Osa DNS:n ylläpitoa PTR-tietueiden luominen käänteiskyselyjen hoitamiseksi.

Kun nimipalvelin käsittelee **rekursiivista kyselyä**, voi olla tarpeen lähettää useita kyselyitä luotettavan vastauksen saamiseksi. Nimipalvelin tallentaa välimuistiinsa kaiken sen tiedon, minkä se vastaanottaa. Säilytysajan pituus määräytyy sen mukaan, mikä aika vastaanotetun tiedon yhteydessä on mainittu. Tätä arvoa kutsutaan nimellä **Time To Live** (TTL). Nimipalvelimen ylläpitäjä määrittelee tietojen TTL-ajan. Mitä pienempi arvo, sen paremmin tiedot pysyvät ajan tasalla muissa palvelimissa - toisaalta tällöin myös pavelinten kuormitus kasvaa.

Kun tiedot tallennetaan nimipalvelimen välimuistiin, se alkaa pienentää TTL-arvoa alkuperäisestä arvosta niin, että tietää milloin välimuistissa oleva tieto on aika poistaa. Jos palvelin palauttaa vastauksena välimuistissa olevaa tietoa, se välittää jäljellä olevan TTL-arvon kysyvälle tietokoneelle. Asiakkaat käyttävät myös välimuistia ja ottavat huomioon TTL-ajan.

DNS:n asetukset

DNS-palvelinta konfiguroidaan perinteisesti useiden eri tiedostojen avulla.

DB-tiedostot

Verkkoaluenimi määrittelee yhden kokonaisuuden DNS-nimiavaruudessa. Kukin kokonaisuus koostuu sarjasta **resurssitietueita** (*Resource record*), jotka yhdessä muodostavat verkkoalueeseen liittyvän informaation. Resurssitietueet tallennetaan tiedostoihin, joita nimitetään **DNS-tietokannoiksi** (*DNS database files*) tai lyhyemmin **DB-tiedostoiksi**. Tyypilliseen DNS-järjestelmään kuuluvat seuraavat DB-tiedostot:

Nimi	Selitys
DB.DOMAIN	Tiedosto, jonka avulla koneennimiä muunnetaan IP-osoitteiksi. Jos verkkoalueesi on esimerkiksi SPECTRE.COM, tämän tiedoston nimi on DB.SPECTRE.COM
DB.ADDR	Tiedosto, jonka avulla muunnetaan IP-osoitteita koneennimiksi. Jos C-luokan verkko-osoitteesi on 192.138.204.0, tämän tiedoston nimi on DB.192.138.204
DB.CACHE	Tämä tiedosto on käytännössä sama kaikilla DNS-palvelimilla. Se on pakollinen tiedosto, joka sisältää juuritason nimipalvelimien nimet ja osoitteet
DB.127.0.0	Tämä tiedosto on käytännössä sama kaikilla DNS-palvelimilla. Se on pakollinen tiedosto, jonka avulla selvitetään loopback-osoitteeseen kohdistettuja kyselyitä

Näiden tiedostojen nimet vaihtelevat ja riippuvat DNS-palvelimen konfiguraatiosta. Windows NT 4.0:n DNS-palvelin ei käytä yllä mainittuja nimiä oletusarvoisesti, mutta se voidaan asettaa käyttämään niitä, jos DB-tiedostoja on tarpeen siirtää toiselta DNS-palvelimelta.
Perinteisesti DNS-palvelinten asetustiedot ovat olleet tekstitiedostossa nimeltä **Boot**. Windows NT:n DNS-palvelin voi käyttää joko **Boo**t-tiedostoa tai järjestelmärekisteriä. Valinta tehdään **DNS Managerissa**.

Resurssitietueet

Resurssitietueiden järjestys DB-tiedostojen sisällä ei ole erityisen tärkeä DNS:n tai asiakkaiden kannalta. Resurssitietueissa on seuraavanlaista informaatiota:

Nimi	Selitys
OWNER	Sen verkkoalueen nimi, josta resurssitietue löytyy
TYPE	Tietueen sisältämä resurssityyppi
CLASS	Käytettävä protokollaperhe. Tämä arvo on lähes aina IN internet-järjestelmässä. Toinen RFC:ssä 1034 määritelty arvo on CH Chaos-järjestelmälle, jota kokeiltiin MIT:ssä
TTL	Time To Live. 32-bittinen kokonaisluku joka ilmoittaa sekunneissa, kuinka kauan tämän tietueen tiedot voidaan pitää välimuistissa
RDATA	Tyypiltään vaihteleva resurssidata, joka edustaa tyypin esittämää informaatiota. Esimerkiksi osoitetietueessa tämän arvo on 32-bittinen IP-osoite, joka edustaa tietueessa määriteltyä konetta

Resurssitietueet on koodattu paketeissa binaarimuotoon DNS:n nimihauissa ja vastauksissa. Tietokantatiedostoissa useimmat tiedot on esitetty yhden rivin tekstiviitteinä. Jos viite ulottuu useammalle riville, se voidaan rajata sulkuihin, vaikkakin useissa DNS-toteutuksissa ainoastaan **SOA-tietue** (*Start Of Authority*) voi ulottua useammalle kuin yhdelle riville. Luettavuuden parantamiseksi käytetään usein tyhjiä rivejä ja kommentteja. DNS-palvelin ei ota tällaisia rivejä huomioon. Kommentti alkaa aina puolipisteellä (**;**) ja päättyy rivinvaihtoon.

Esimerkkitietue voisi näyttää tältä:

```
WS4.ZULU.FISHWARE.COM  3600        A      IN      130.9.63.6
```

Kukin resurssitietue alkaa omistajalla (**WS4.ZULU.FISHWARE.COM**). Jos omistajaa ei ole mainittu, omistajana pidetään edellisen tietueen omistajaa. Omistajaa seuraa **TTL** (3600 = 1 tunti), **tyyppi** (A = osoitetietue), **luokka** (IN = internet) ja **RDATA** (resurssidata, tässä IP-osoite). Jos TTL-arvoa ei ole, sen oletetaan olevan sama kuin SOA:n TTL-arvo.

Resurssitietuetyypit

Resurssitietueita voi olla useita eri tyyppisiä. **RFC 1034** määrittelee seitsemän tyyppiä, jotka ovat:

Tyyppi	Kuvaus
SOA	Määrittelee valtuutusvyöhykkeen alun
A	Koneen osoite
NS	Vyöhykkeen valtuutettu nimipalvelin
PTR	Osoitin toiseen nimiavaruuden kohtaan
CNAME	Aliasnimi
MX	Määrittelee verkkoalueen postinvälitystavan (Mail eXchange)
HINFO	Konetiedot. Käytetään usein koneen prosessorin ja käyttöjärjestelmän tunnistamiseen

RFC 1035 lisää listaan seuraavat resurssityypit:

Tyyppi	Kuvaus
MB	Yhdistää tietyn DNS-koneen tiettyyn postilaatikkoon. Käytetään resurssitietueiden MG, MR ja MINFO yhteydessä
MG	Määrittelee postilaatikon, joka kuuluu DNS-verkkoaluenimen määrittelemään postiryhmään (postituslistaan). Käytetään resurssitietueiden MB, MR ja MINFO yhteydessä
MINFO	Määrittelee postilaatikon, joka on vastuussa postituslistasta tai postilaatikosta. Käytetään resurssitietueiden MB, MG ja MR yhteydessä
MR	Määrittelee toisen nimen postilaatikolle
TXT	Liittää teksti-informaatiota mihin tahansa DNS-tietokannan kohteeseen

Näiden lisäksi **RFC 1183** määrittelee vielä seuraavat tyypit:

Tyyppi	Kuvaus
AFSDB	Joko Andrew-tiedostojärjestelmän (Andrew File System Cell Database) tai DCE:n (Distributed Computing Environment) nimipalvelimen sijainti
RP	DNS-verkkoalueen tai koneen vastuuhenkilö
X.25	Koneen nimeä vastaava X.121-osoite. Käytetään RT-resurssitietueen yhteydessä
ISDN	Koneen nimeä vastaava ISDN-osoite. Käytetään RT-resurssitietueen yhteydessä
RT	Välittäjäkone, joka reitittää paketteja kohdekoneeseen

Myös **RFC 1886** määrittelee yhden resurssitietuetyypin:

Tyyppi	Kuvaus
AAAA	Erityinen osoitetietue, jossa määritellään laitenimeä vastaava Ipv6-osoite

Microsoftilla on lisäksi pari omaa tyyppiä:

Tyyppi	Kuvaus
WINS	Microsoftin DNS voi käyttää WINS-palvelinta DNS-nimen koneosan selvittämiseen. Tällöin DNS-palvelin voi kuulua useampaan kuin yhteen vyöhykejuureen (Zone root)
WINS-R	Käänteinen WINS-selvitys. Käytetään käänteisselvitystiedostossa, kun koneen nimi halutaan selvittää IP-osoitteen perusteella. WINS-palvelin selvittää koneen nimen lähettämällä NBTSTAT-kyselyn

Microsoftin DNS on täysin yhteensopiva RFC:iden 1034, 1035 ja 1183 kanssa.

Boot

Vaikka Boot-tiedostoa ei olekaan varsinaisesti määritelty yhdessäkään RFC:ssä eikä sen tarvitse olla RFC-yhteensopiva, se on olennainen osa DNS:ää ja osa BIND:n DNS-toteutusta. Windows NT 4.0:n DNS voidaan myös asettaa käyttämään Boot-tiedostoa, jos ylläpitoon jostain syystä soveltuu paremmin tekstitiedostojen editointi kuin **DNS Managerin** käyttö. Tiedosto kontrolloi DNS-palvelimen käynnistystä. Se sisältää komentoja, joiden on oltava rivin alussa ilman yhtään edeltävää välilyöntiä. Tiedostossa voidaan käyttää seuraavia komentoja:

- **Directory-komento** määrittelee hakemiston, jossa ovat Boot-tiedostossa mainitut tiedostot

- **Cache-komento** määrittelee tiedoston, jota DNS-palvelu käyttää ottaakseen yhteyden juuritason DNS-palvelimiin. Tämän komennon on oltava Boot-tiedostossa, ja tämän komennon määrittelemän tiedoston on oltava olemassa

- **Primary-komento** määrittelee verkkoalueen, jolle tämä palvelin on **valtuutettu** palvelin, sekä resurssitietueet sisältävän tietokannan (eli vyöhyketiedoston, *Zone file*). Boot-tiedostossa voi olla useita primary-komentoja

- **Secondary-komento** määrittelee verkkoalueen, jolle tämä palvelin on valtuutettu palvelin sekä niiden päänimipalvelinten (Master server) IP-osoitteet, joista tämä palvelin voi noutaa vyöhyketiedot. Määrittelee myös paikallisen tiedoston tämän vyöhykkeen välimuistille. Boot-tiedostossa voi olla useita secondary-komentoja.

CACHE-tiedosto

Cache-tiedostossa on konetiedot, joita tarvitaan oman verkkoalueen ulkopuolisten kyselyiden ratkaisemiseen. Tiedosto sisältää juuritason nimipalvelinten nimet ja osoitteet. Internet-käytössä Windows NT 4.0:n DNS-palvelimen mukana tuleva tiedosto kelpaa aluksi hyvin, koska siinä on kaikkien internetin juuritason nimipalvelinten tiedot. Jos verkko ei ole yhteydessä internettiin, tiedosto pitää korvata sellaisella, jossa on oman verkon juuritason palvelinten tiedot.

Uusimman internetin cache-tiedoston löydät osoitteesta **ftp://rs.internic.net/domain/named.cache**.

Käänteisselvitystiedosto

Reverse Lookup -tiedostoa käytetään käänteiseen DNS-selvitykseen, jossa IP-osoite muunnetaan vastaavaksi koneennimeksi. Tiedosto on ikään kuin vyöhyketiedosto vyöhykkeelle IN-ADDR.ARPA.

Osoitintietueet mahdollistavat staattisen IP-osoitteiden liittämisen koneennimiin käänteisselvitysvyöhykkeen (*Reverse Lookup Zone*) sisällä. IP-osoitteet kirjoitetaan takaperin ja niiden perään lisätään teksti IN-ADDR.ARPA, jotta osoitintietue olisi täydellinen. Esimerkiksi osoitetta 130.9.63.5 vastaavan nimen löytäminen vaatii PTR-kyselyä osoitteella 5.63.9.130.IN-ADDR-ARPA.

Windows NT 4.0 DNS-palvelin

Windows NT Server 4.0 sisältää DNS-palvelimen, joka on RFC-yhteensopiva ja toimii Windows NT-palveluna.

Koska se on RFC-yhteensopiva, se käyttää DNS-vyöhyketiedostoja ja tukee kaikkia standardeja resurssitietuetyyppejä. Sitä voidaan käyttää yhdessä muiden DNS-palvelinten kanssa ja sen mukana tulee **NSLOOKUP**-apuohjelma. Microsoftin DNS-toteutuksessa on myös monia parannuksia ja laajennuksia alkuperäiseen DNS:ään verrattuna, kuten dynaaminen päivitys WINS-integroinnin avulla ja **DNS Manager**-hallintaohjelma.

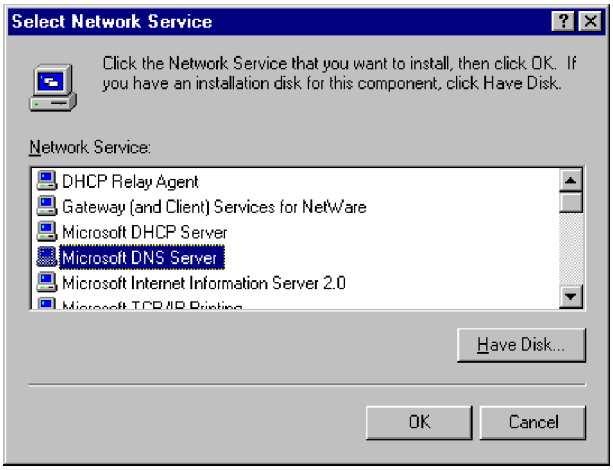
Windows NT:n DNS mahdollistaa myös täysin dynaamisen ylläpidon. Microsoft-tietokoneet voidaan poistaa staattisista DNS-vyöhyketiedostoista, koska DNS toimii yhteistyössä WINS:n kanssa. Jos esimerkiksi Microsoft-työasema haluaa ottaa yhteyden HTTP-palvelimella olevaan WWW-sivuun ja HTTP-palvelin käyttää DHCP/WINS-yhdistelmää, asiakas voi lähettää kyselyn DNS-palvelimelle joka puolestaan lähettää kyselyn WINS-palvelimelle. Tämä ratkaisee kyselyn, ja lopulta vastaus palautetaan asiakkaalle. Ilman WINS-integrointia ei olisi luotettavaa keinoa selvittää DHCP:n avulla jaettuja IP-osoitteita.

Ennen kuin asennat DNS-palvelun Windows NT:hen, tarkista että TCP/IP:n asetukset ovat kohdallaan. Erityisesti DNS-asetukset on syytä tarkistaa, koska DNS-palvelin käyttää oletuksena TCP/IP:n DNS-välilehdellä olevia koneen ja verkkoalueen nimiasetuksia. Jos verkkoalueen nimi ja koneen nimi ovat olemassa silloin, kun luot vyöhykkeen, DNS luo automaattisesti vyöhykkeen SOA-tietueen (*Start Of Authority*) ja lisää A- sekä NS-tietueet sille palvelimelle, jolla DNS-palvelua ajetaan.

Jos koneen ja verkkoalueen nimeä ei ole asetettu, DNS luo ainoastaan SOA-tietueen.

Tee asennus seuraavasti:

1) Aloita asennus Ohjauspaneelin **Network**-valintaikkunan **Services**-välilehdellä painamalla **Add**-painiketta. Valitse **Microsoft DNS Server** ja napauta **OK**.



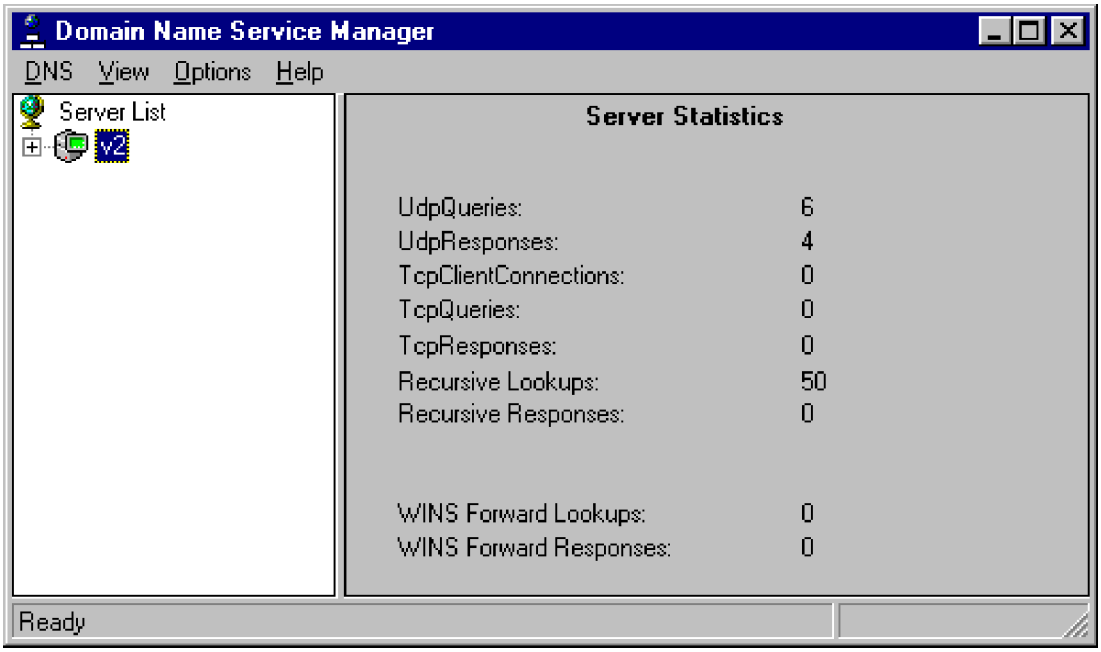
2) Käynnistä palvelin uudelleen. DNS-palvelu käynnistyy automaattisesti uudelleenkäynnistyksen yhteydessä.

Microsoftin DNS-palvelin osaa käyttää minkä tahansa toisen valmistajan DNS-palvelimen asetustiedostoja, jos ne ovat RFC-yhteensopivia. Siirtääksesi tällaiset tiedostot NT-käyttöön sinun tulee vai kopioida ne DNS-hakemistoon (oletuksena %SYSTEMROOT%\SYSTEM32\DNS) ja muokata joko **Boot**-tiedostoa tai rekisteriä niin, että DNS-palvelin osaa käyttää uusia tiedostoja.

Domain Name Service Manager

Windows NT 4.0:n DNS-palvelimen mukana tulee DNS Manager.

Kun DNS-palvelu on käynnissä, palvelimeen voidaan lisätä vyöhykkeitä ja verkkoalueita. Aluksi **DNS Manager** näyttää sen palvelimen nimen, jolle palvelu on asennettu; jos ei, lisää palvelin **Server List**-luetteloon valinnalla **DNS** | **New Server**. Kaksoisnapauta palvelimen nimeä nähdäksesi tilastotiedot sekä määritellyt vyöhykkeet.

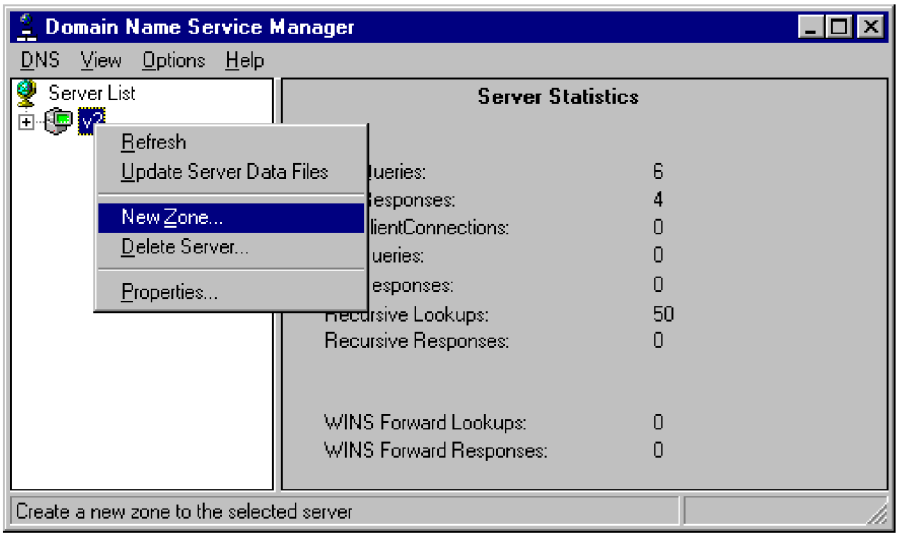


Koska DNS-palvelimella ei ole mitään alkutietoja käytössä olevasta verkosta, se asentuu pelkkänä internetin välimuistipalvelimena. Tämä tarkoittaa, että palvelimella on tiedot ainoastaan internetin juuritason nimipalvelimista. Useimmiten palvelimelle pitää määritellä lisää tietoja, jotta se toimisi kunnolla.

DNS-verkkoalueiden ja vyöhykkeiden lisääminen

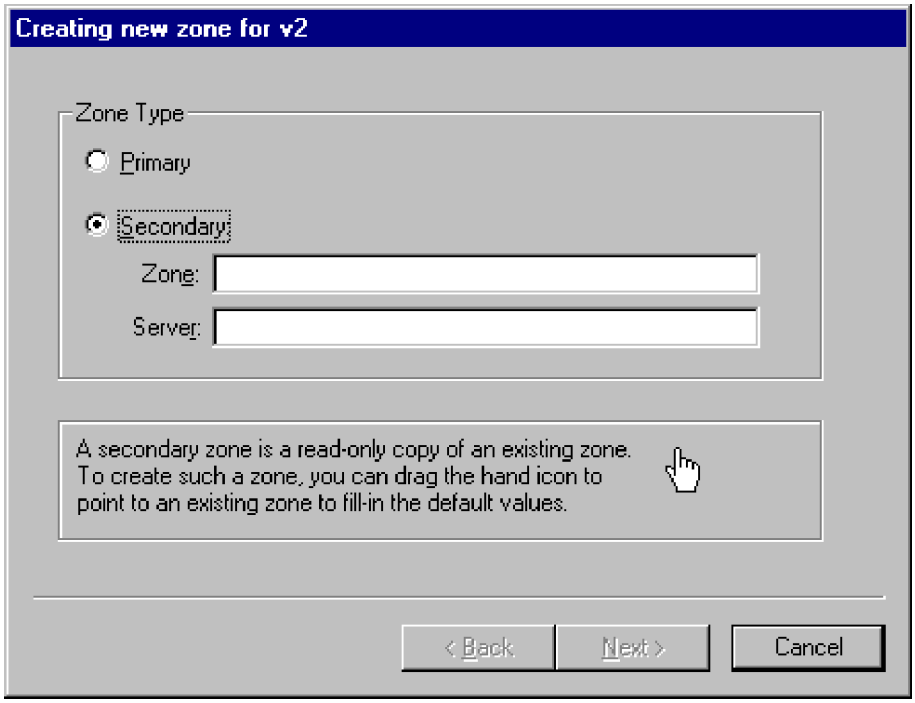
Ensimmäinen vaihe konfiguroinnissa on päättää DNS-verkkoaluehierarkiasta ja vyöhykkeistä. Kun nämä päätökset on tehty, voidaan tiedot syöttää DNS-palvelimelle DNS Managerin kautta.

Koska DNS-informaatio ryhmitellään vyöhykkeittäin, ensin on luotava vyöhyke. Valitse hiiren pikavalikosta palvelimen kohdalla **New Zone**.



Näytölle tulee ikkuna, jossa voit valita, onko kyseessä **ensi**- vai **toissijainen** vyöhyke. Ensisijaisen vyöhykkeen tiedot tallennetaan paikallisesti, toisijaisen haetaan joltakin muulta palvelimelta. Jos haluat luoda ensisijaisen vyöhykkeen, tässä vaiheessa ei tarvitse määritellä mitään tarkempia tietoja.

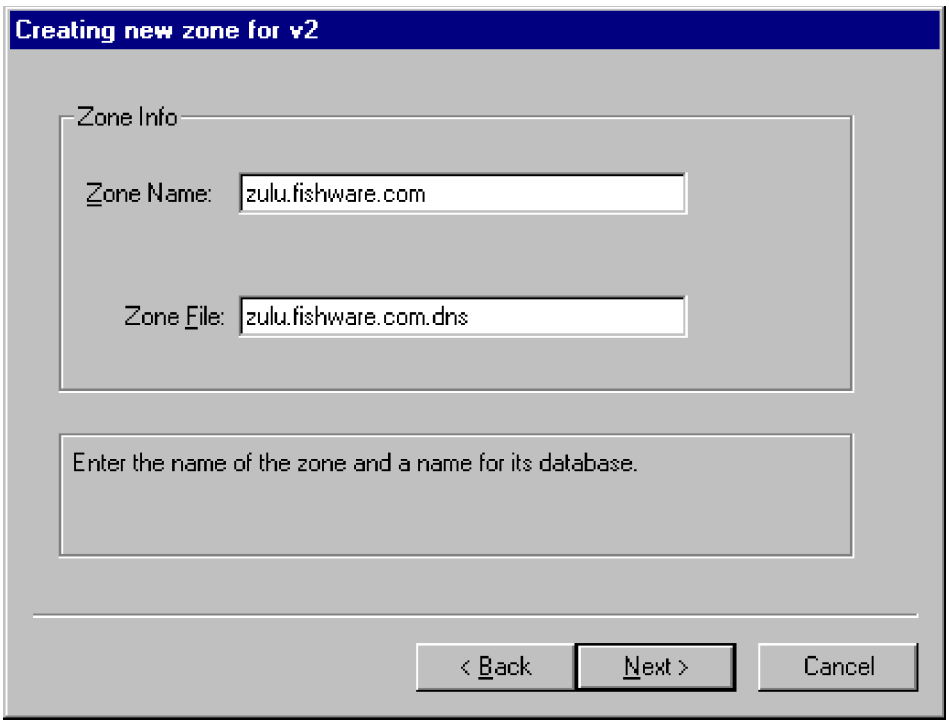
Jos haluat luoda toissijaisen vyöhykkeen, pitää sinun määritellä vyöhykkeen ja päänimipalvelimen nimet.



Toissijaisen vyöhykkeen luominen on helppoa, jos käytät ikkunassa olevaa käsikuvaketta. Järjestele näyttö ja palvelimien lista siten, että ensisijainen vyöhyke on näkyvissä. Vedä hiirellä käsi DNS Manager -ikkunaan halutun palvelimen ylle. DNS Manager täyttää tällöin automaattisesti toissijaisen vyöhykkeen nimi- ja palvelintiedot.

Vyöhykkeen ja vyöhyketiedoston nimi

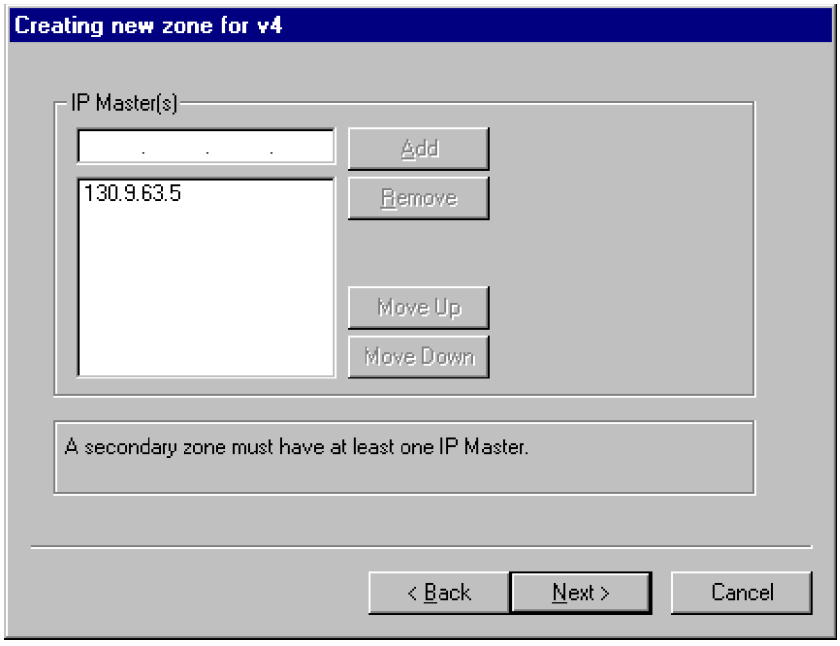
Sekä ensi- että toissijaista vyöhykettä varten täytyy määritellä vyöhykkeen nimi ja vyöhyketiedosto paikalliselle palvelimelle. Tämä määrää, kuinka vyöhyke näkyy DNS Managerissa ja millä tiedostonimellä se tallennetaan.



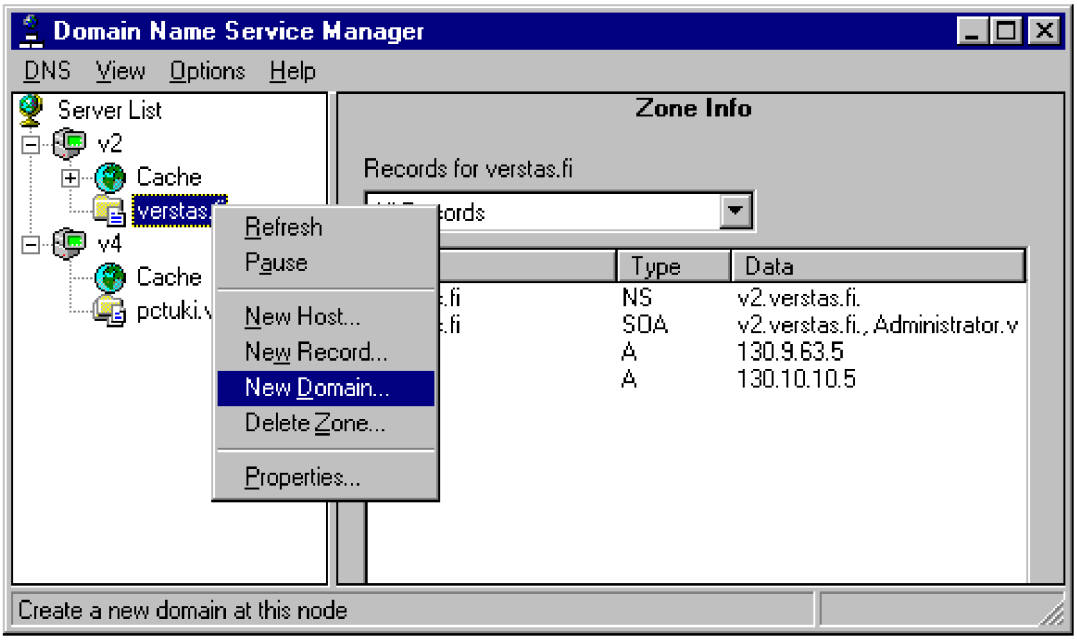
Kun vyöhykkeelle on annettu nimi, DNS Manager luo oletustiedostonimen. Windows NT:n DNS-palvelimella tämä on VYÖHYKENIMI.DNS, kun taas muilla palvelimilla nimi on DB.VYÖHYKENIMI.

Jos kyseessä on toissijainen vyöhyke, nimen tulisi olla sama kuin **päänimipalvelimen** vyöhykenimen. Jos vyöhyketiedosto on jo ennestään olemassa DNS-hakemistossa (jonkin toisen DNS-ohjelmiston jäljiltä, esimerkiksi **MetaInfo**), DNS Manager tuo vanhassa tiedostossa olevat viitteet automaattisesti vyöhykkeen luomisen yhteydessä.

Kun luot toissijaisen vyöhykkeen, sinun pitää määritellä päänimipalvelimen IP-osoite. Toissijainen nimipalvelin hakee nimitiedot tältä palvelimelta. IP-osoitteen määrittelyn jälkeen vyöhyke lisätään DNS-hierarkiaan. Paina lopuksi **Finish**.



Jos on tarpeen lisätä useampia vyöhykkeitä, tee kuten edellä. Kun kaikki vyöhykkeet on lisätty, vyöhykkeiden alaisuuteen voidaan lisätä verkkoalueita. Napauta tällöin haluamaasi vyöhykettä ja valitse hiiren pikavalikosta komento **New Domain**.

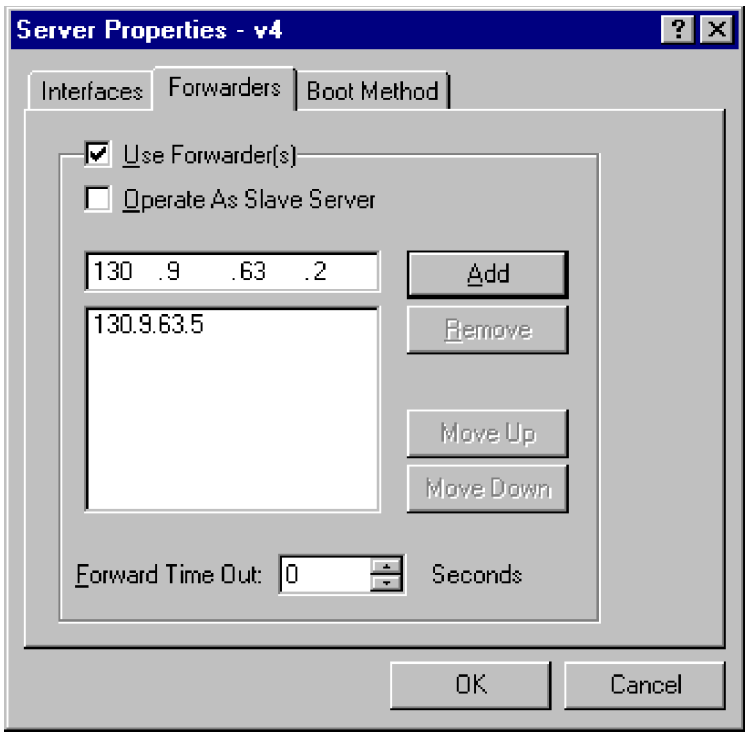


Kirjoita avautuvaan ikkunaan uuden verkkoalueen nimi ja napauta **OK**. Jos on tarpeen lisätä useampia verkkoaluetasoja, luo muut verkkoalueet toisten verkkoalueiden alle vastaavalla tavalla.

Samalla tavalla voidaan lisätä myös uusia tietokoneita tai resurssitietueita mihin tahansa kohtaan DNS-hierarkiassa.

Välittäjien konfigurointi

Kun haluat tehdä DNS-palvelimesta välittäjäpalvelimen, avaa haluamastasi palvelimesta ominaisuudet ja valitse **Forwarders**-välilehti.

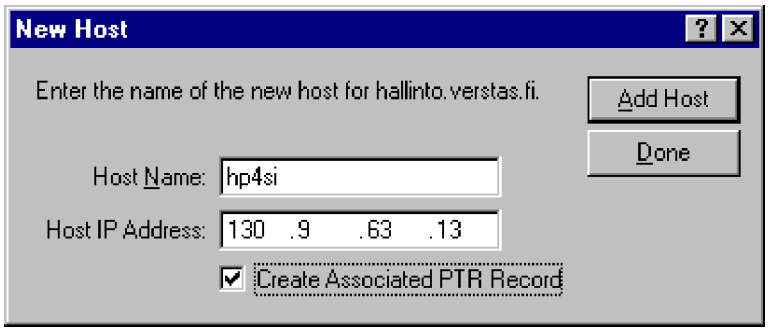


Valitse **Use Forwarder(s)** ja lisää yksi tai useampia välittäjäpalvelinten IP-osoitteita. Jos haluat, että tämä palvelin toimii välittäjien orjana, rastita ruutu **Operate As Slave Server**.

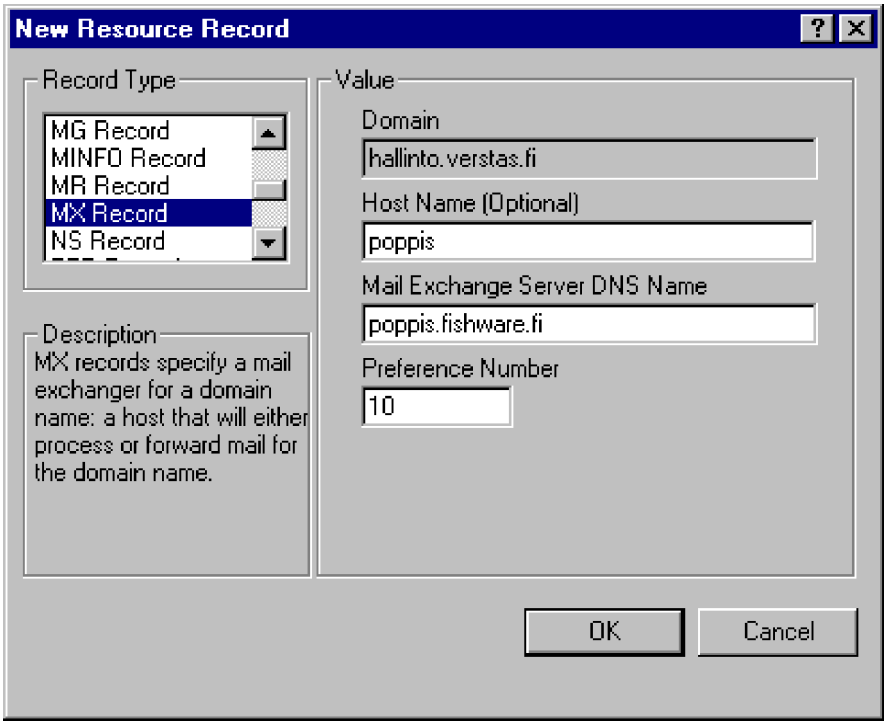
Tällöin nimipalvelin ei yritäkään ratkaista pyyntöä itse, vaan **toimittaa sen suoraan** välittäjälle. Jos välittäjä ei löydä vastausta, nimipalvelin palauttaa asiakkaalle virheen.

Tietueiden lisääminen

Kun olet lisännyt vyöhykkeet ja verkkoalueet, voit ryhtyä lisäämään resurssitietueita. Lisätäksesi tietueen valitse vyöhyke tai verkkoalue ja valitse pikavalikosta **New Host** tai **New Record**.



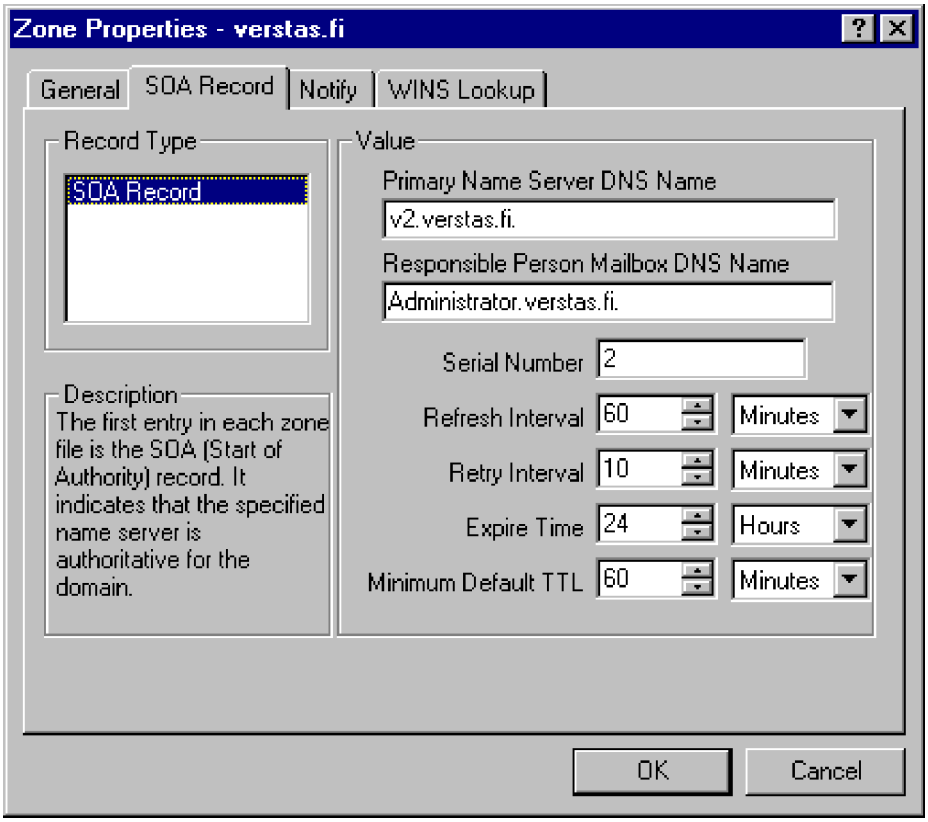
Kun valitset komennon **New Host**, voit kirjoittaa nimen ja IP-osoitteen. Valittavissa on myös ruutu, jonka rastittamalla voit luoda automaattisesti osoitintietueen (*PTR*) käänteisselvitystä varten. Tässä ikkunassa voit luoda vain A-tietueita (*Address*).



Jos valitset **New Record**, voit valita millaisen resurssitietueen haluat luoda. Kun valitset **Record Type**-listasta jonkin tietuetyypin, **Value**-osaan tulevat näkyviin kyseiseen tietuetyyppiin liittyvät asetukset. Napauta **OK** lisätäksesi tietueen.

SOA-asetusten muuttaminen

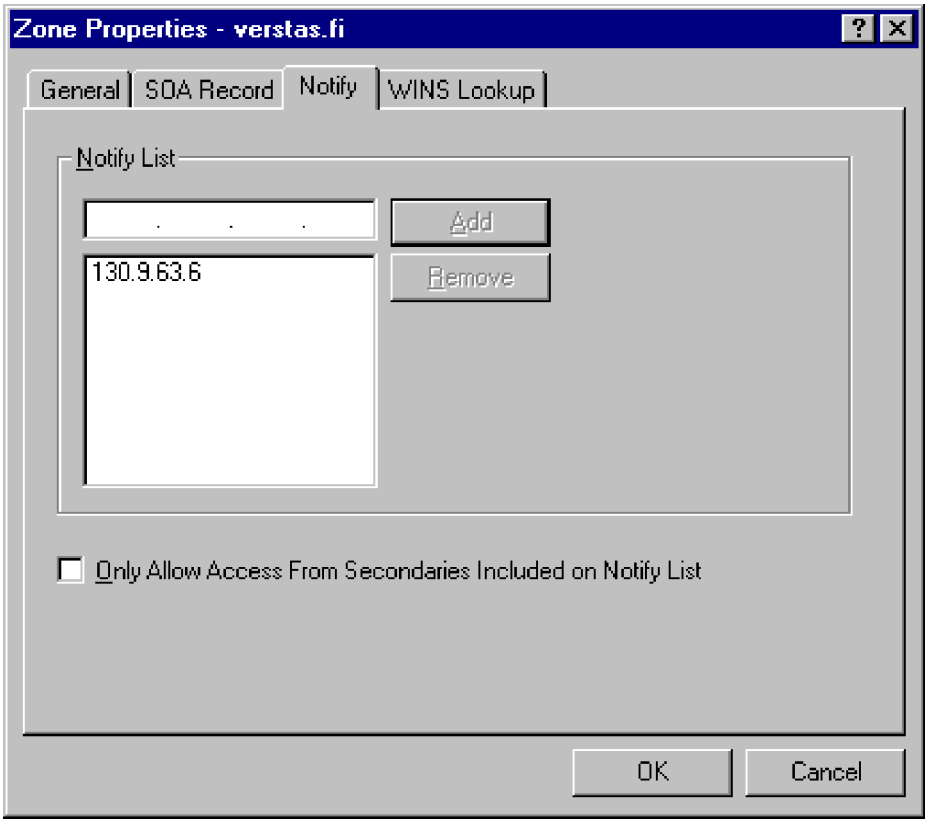
Kun haluat määritellä vyöhykkeen SOA-tietueen (*Start Of Authority*) ominaisuudet, avaa DNS Managerissa haluamasi vyöhykkeen ominaisuudet ja **SOA Record** -välilehti.



Kaikkia näkyviä ominaisuuksia ei voi muuttaa, ja ne tallentuvat vyöhyketiedoston SOA-tietueeseen.

Ilmoituslista

Vyöhykesiirto tehdään aina palvelimen käynnistyessä sekä määräajoin sen jälkeen, mikäli vyöhyketiedot ovat muuttuneet. Jos haluat, että vyöhykesiirrot tehdään aina heti muutosten tapahduttua, voit lisätä ensisijaisen vyöhykkeen ilmoituslistaan (*Notify list*) niiden toissijaisten nimipalvelinten IP-osoitteet, joille haluat palvelimen lähettävän ilmoituksen. Kun vyöhyketiedosto muuttuu, ensisijainen palvelin lähettää listassa oleville toissijaisille palvelimille DNS-muutosilmoituksen. Tällöin ilmoituksen vastaanottaneet nimipalvelimet voivat päivittää tietonsa heti, eikä niiden tarvitse odottaa, että määräaika tulee täyteen.



Avaa haluamasi vyöhykkeen ominaisuusikkuna ja valitse **Notify**-välilehti. Kirjoita listaan vyöhykkeen niiden toissijaisten nimipalvelinten IP-osoitteet, joille haluat ilmoitusten lähtevän.

Jos valitset **Only Allow Access from Secondaries Included on Notify List**, ensisijainen nimipalvelin hyväksyy ainoastaan listassa olevien palvelinten vyöhykesiirtopyynnöt.

Käänteisselvitys

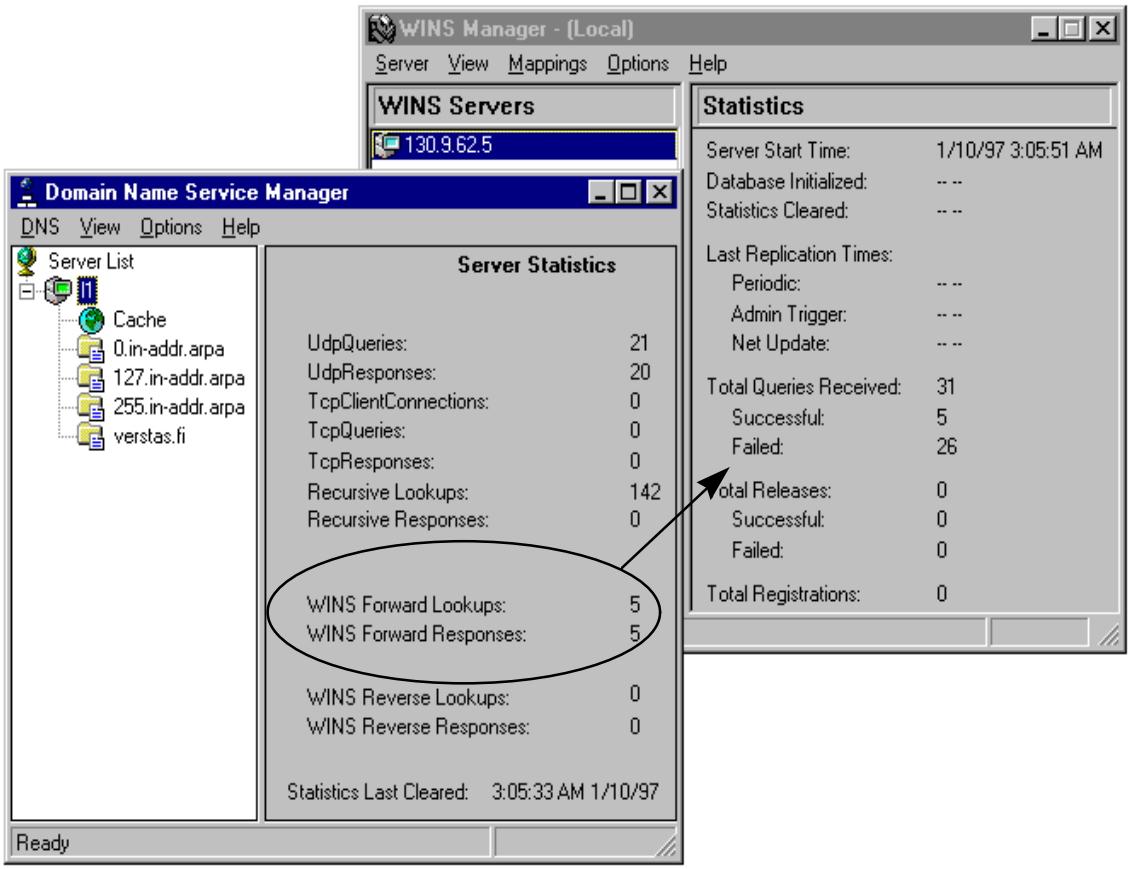
Jotta koneen IP-osoitteen perusteella olisi mahdollista selvittää koneen nimi, täytyy luoda käänteisselvitysvyöhyke jokaiselle verkolle, jossa DNS-tietokannan koneita on. Tämä tehdään periaatteessa samalla tavalla kuin minkä tahansa vyöhykkeen lisääminen (vyöhykkeen nimen tulee kuitenkin olla RFC 1035:n mukainen). Tämän vyöhykkeen alkupiste on **IN-ADDR.ARPA** ja sen rakenne noudattaa internetin osoiterakennetta.

DNS:n ja WINS:n integrointi

Windows NT 4.0:n DNS-palvelin mahdollistaa WINS:n ja DNS:n yhteistoiminnan. Se kykenee myös välittämään ratkaisemattomat nimikyselyt edelleen WINS-palvelimelle.

Tämä tapahtuu käyttäjän huomaamatta, eikä asiakkaan tarvitse tietää, mikä nimipalvelu pyynnön lopulta ratkaisee. Jos käytät sekä DNS:ää että WINS:ää Windows NT -pohjaisessa verkossa, voit sekä muuntaa IP-osoitteita käyttäjäystävällisiksi NetBIOS- tai DNS-nimiksi että suorittaa muunnoksen päinvastaiseen suuntaan.

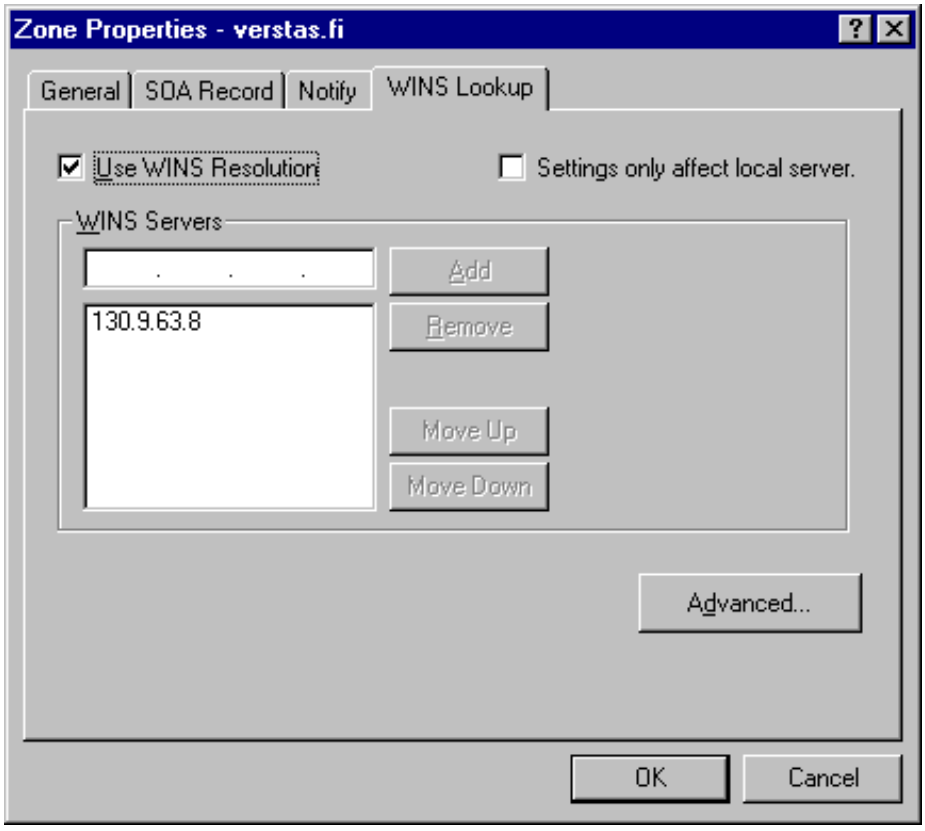
Tällöin menetelmää kutsutaan dynaamiseksi, ja siinä yhdistyvät DNS- ja WINS-palvelun ominaisuudet siten, että DNS selvittää toimialueen nimen ylemmät kerrokset ja WINS hoitaa lopullisen selvityksen. Kyselyn lähettävä tietokone ei edes huomaa, että itse asiassa WINS-palvelu suorittaa lopullisen selvityksen.



Windows NT -koneen **Workstation**-palvelu vastaa kyseisen tietokoneen nimen rekisteröimisestä WINS-palvelun avulla. Oletuksena Workstation-palvelu käynnistyy automaattisesti NT:n käynnistyksen yhteydessä eikä asetusta tule muuttaa.

Jos esimerkiksi palvelin sammutetaan, niin DNS-palvelin ei enää voikaan selvittää tietokoneen nimeä WINS-palvelun avulla.

DNS Managerissa WINS-asetus on osa vyöhykkeen ominaisuuksia. Avaa vyöhykkeen ominaisuudet ja **WINS Lookup** -välilehti. Ota WINS-selvitys käyttöön rastittamalla ruutu **Use WINS Resolution**. Kirjoita WINS-palvelinten IP-osoitteet listaan.



Windowsin **UNC** (*Uniform Naming Convention*)-menetelmä tukee myös DNS:n toimialueen nimiä. UNC-resurssit osoitetaan muodossa **palvelin\resurssi**. Aiemmin palvelin oli vain sen palvelimen **NetBIOS-nimi**, jossa resurssi sijaitsi, mutta nyt UNC-nimen palvelimen osassa voi käyttää **DNS-toimialueen nimeä** tai **IP-osoitetta**. Jotta DNS tukisi UNC-nimiä, on DNS otettava käyttöön nimiselvityksessä.

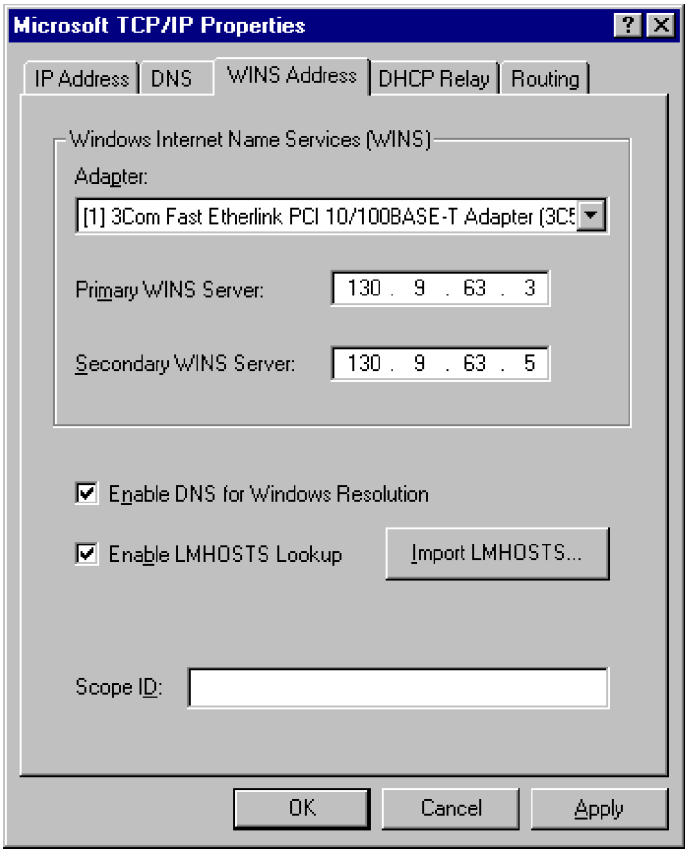
Isäntätiedostot

ASCII-muotoisia **LMHOSTS**- ja **HOSTS**-isäntätiedostoja (*host file*) voidaan käyttää määrittämään tietokonenimet ja IP-osoitteet verkoissa, joissa ei käytetä DNS- ja/tai WINS-palvelua:

- HOSTS-tiedostoa voidaan käyttää kuten paikallista DNS:ää
- LMHOSTS-tiedostoa voidaan käyttää kuten paikallista WINS-palvelua.

Tiedostoja kutsutaan myös **isäntätaulukoiksi** (*host table*). Windows NT:n **Winnt\System32\Drivers\Etc**-hakemistoon on TCP/IP:n asennusvaiheessa tallennettu mallit LMHOSTS- ja HOSTS-tiedostosta, tiedostojen tarkennin on **SAM: LMHOSTS.SAM** ja **HOSTS.SAM**. Tiedostoja voi muokata esimerkiksi **Muistiolla** (Notepad) tai **EDIT**:illä. Muista tallentaa ne ilman SAM-tarkenninta!

Käyttöönotto tehdään **WINS-osoite** (WINS Address)-välilehdessä valitsemalla **Enable LMHOSTS Lookup**.



DNS:n valinta ottaa käyttöön **HOSTS**-tiedoston ja **LMHOSTS**:in valinta **LMHOSTS**-tiedoston.

HOSTS-tiedostolla ratkaistaan IP-osoitteiden ja DNS-tietokonenimien vastaavuudet. HOSTS-tiedostoa käyttävät Windows Sockets -sovellukset TCP/IP-isäntänimien selvittämiseen. Kirjoita ensin IP-osoite ja sitten tietokonenimi. Esimerkiksi:

```
# VERSTAS-DOMAIN HOSTS FILE
#
# Author: JK & HA 20.7.97 19:93
#
127.0.0.1       localhost
130.9.63.8      v1.verstas.fi
130.9.63.9      v2.verstas.fi
130.9.63.7      v6.verstas.fi
```

Huomaat nopeasti **HOSTS**-tiedoston tarpeellisuuden, jos käytät vaikkapa Internet-selaimia ja käytössäsi *ei* ole DNS:ää. Voit kokeilla vaikka omassa verkossasi asentamalla WWW-palvelinohjelmiston (*HTTP Server, HTTP Daemon*) sopivaan palvelimeen, ja kun yrität saada yhteyttä WWW-palvelimeen Internet-selaimellasi, se ei välttämättä onnistu. Kokeile tällöin tietokoneen lisäämistä **HOSTS**-tiedostoon ja yritä uudelleen.

Voit käyttää kokeilussa vaikka Windows NT 4.0-työaseman **Vertais-WWW-palvelun** (Peer Web Services) veppipalvelinta.

LMHOSTS-tiedostolla määritetään **NetBIOS-tietokonenimien** ja **IP-osoitteiden vastaavuudet. LMHOSTS**-tiedostoa käyttävät **NetBIOS over TCP/IP**-sovellukset Microsoft-verkkoympäristössä tietokonenimien selvittämiseen. Esimerkiksi **NET USE** -komennot käyttävät **NetBIOS over TCP/IP**:tä.

LMHOSTS-tiedostoa käytetään tyypillisesti pienissä verkoissa ja aliverkoissa, joissa ei ole omaa WINS-palvelua. **LMHOSTS**-tiedosto luetaan, kun WINS:iin tai yleislähetyksiin perustuva nimiselvitys ei onnistu. Selvitetyt nimet tallennetaan mikron **välimuistiin** myöhempää käyttöä varten ja välimuisti alustetaan aina mikron käynnistyksen yhteydessä.

Kun jokin nimi on selvitettävä, sitä etsitään ensin välimuistista - jos nimeä ei ole välimuistissa, Windows NT -työasema lähettää yleislähetyskyselyn. Jos siihen ei tule vastausta, luetaan **LMHOSTS**-tiedostoa - ja jos

tietokonetta ei löydy **LMHOSTS**-tiedostostakaan, nimi jää selvittämättä ja näyttöön tulee **virheilmoitus**.

Verkoissa, joissa ei ole **WINS**-palvelua, voidaan käyttää **yleislähetyksiin** perustuvaa nimiselvitystä. Tällöin TCP/IP-verkon resurssit voidaan paikantaa dynaamisesti nimen mukaan. **WINS** on kuitenkin ensisijainen nimiselvitystapa, jos se on käytössä verkkojen välisissä yhteyksissä - tällöin nimiselvitykseen ei tarvita yleislähetyskyselyjä, sillä **LMHOSTS**-tiedostoa voi käyttää sekä WINS:in kanssa että ilman.

LMHOSTS-tiedostoa kannattaakin käyttää joko **pienissä verkoissa** tai käytettäessä palvelimia verkoista, jotka **eivät ole WINS-tietokannassa**, koska yleislähetyksiin perustuvia nimikyselysanomia ei lähetetä paikallisen aliverkon ulkopuolelle. Nimet voidaan kuitenkin selvittää yleislähetysalueen ulkopuolelle, **jos tietokoneen nimi** ja sen **IP-osoite on määritetty LMHOSTS-tiedostossa**.

Koska Windows-mikro ylläpitää välimuistia tietokonenimistä ja IP-osoitteista, selvitettäessä jotakin nimeä sitä etsitään ensin välimuistista, sitten lähetetään yleislähetyskysely ja vasta lopuksi luetaan **LMHOSTS**-tiedostoa. Windows NT -mikro käyttää **LMHOSTS**-tiedostoa, jos sen käyttöönotto on määritelty (**Käytä LMHOSTS hakua**):

```
# VERSTAS-DOMAIN LMHOSTS-FILE
#
# Author: JK 13.9.96
#
#
130.9.63.10     v1          #PRE #DOM:VERSTAS    #PDC Verstas
130.9.63.9      ws2             #PRE          #WWW
130.9.63.100    v2              #PRE          #DHCP,BDC
130.9.63.110    v3              #PRE          #WINS,BDC

#BEGIN_ALTERNATE
#INCLUDE \\v1\yht\lmhosts2
#INCLUDE \\v2\yht\lmhosts2
#END_ALTERNATE
```

LMHOSTS-tiedostossa voi olla paljon nimimäärityksiä. LMHOSTS-tiedostossa määritellyt tietokoneet voivat olla:

- Windows NT Workstation -työasemia
- Windows NT Server -palvelimia
- LAN Manager -palvelimia
- Työryhmä-Windows-työasemia tai -palvelimia
- Windows 95 -työasemia tai -palvelimia

Yhteinen nimittäjä näille kaikille on Microsoftin TCP/IP. Kaikkien ympäristöjen palvelimet määritetään LMHOSTS-tiedostossa samalla tavalla. Jos verkossa käytetään NT:n monistuspalvelua (*replikointi*), mutta ei WINS-palvelua, käytettyjen NT-palvelimien LMHOSTS-tiedostossa on oltava kaikkien eri aliverkoissa replikointiin osallistuvien palvelimien nimet.

LMHOSTS-tiedostoa käytetään usein myös pienissä verkoissa, joissa ei ole palvelimia. LMHOSTS-tiedostoa koskevat seuraavat säännöt:

- Jokaisen määrityksen on oltava omalla rivillään
- IP-osoitteen on alettava ensimmäisestä sarakkeesta ja heti sen jälkeen on oltava vastaava tietokonenimi
- IP-osoitteen ja tietokonenimen välissä on oltava ainakin yksi välilyönti tai sarkainmerkki.

Yleensä **#**-merkki aloittaa kommentin. Se voi kuitenkin osoittaa myös erityisiä **avainsanoja**, joita ovat:

#PRE

Lataa määrityksen nimivälimuistiin: oletuksena määritykset eivät lataudu nimivälimuistiin, vaan ne tulkitaan vasta, kun **WINS**- ja **nimikyselysanomat** eivät voi selvittää nimeä. #PRE-avainsana on lisättävä tietokonenimiin, joita käytetään #INCLUDE-riveillä; muussa tapauksessa #INCLUDE-määritys ohitetaan

#DOM:<toimialue>

Liittää määrityksen tiettyyn toimialueeseen; tämä vaikuttaa siihen, miten **selaus (Browser)**- ja **kirjoittautumis (Logon)**-palvelut toimivat TCP/IP-ympäristöissä. Jos haluat #DOM-määrityksen latautuvan nimivälimuistiin, lisää riville #PRE-avainsana

#INCLUDE <tiedostonimi>

Etsii määritetyn tiedoston ja tulkitsee sen kuten paikallisen LMHOSTS-tiedoston. Tiedostonimen voi määrittää **UNC-muodossa** (esim. **V1\PROFILES\LMHOSTS**), jolloin voit käyttää palvelimella olevaa jaettua LMHOSTS-tiedostoa. Jos palvelin ei ole paikallisella yleislähetysalueella, palvelimen nimimääritys on tehtävä ennen **#INCLUDE**-riviä ja se on ladattava nimivälimuistiin avainsanalla **#PRE**

#BEGIN_ALTERNATE

Merkitsee #INCLUDE-lohkon alun. Kyseisen lohkon suoritus onnistuu, jos yhden siihen kuuluvan #INCLUDE-lauseen suoritus onnistuu

#END_ALTERNATE

Merkitsee #INCLUDE-lohkon lopun

\0xnn Esittää tulostumattoman merkin NetBIOS-nimessä. Kirjoita NetBIOS-nimi lainausmerkkeihin ja määritä tulostumattoman merkin heksadesimaaliarvo muodossa \0xnn. Erikoismerkki on merkkijonon viimeinen eli 16. merkki

Esimerkiksi mikron käynnistyksen yhteydessä nimivälimuistiin ladataan LMHOSTS-tiedostosta **vain** ne rivit, joilla on **#PRE-avainsana** (Preload). LMHOSTS-tiedostossa voi olla esimerkiksi seuraavat rivit:

```
193.88.121.67    V5          #Kirjoitinpalvelin
193.88.121.65    V1    #PRE  #Domain Controller
```

Tässä esimerkissä palvelimen V1 määritys ladataan nimivälimuistiin, koska sen jäljessä on annettu avainsana **#PRE**. WfW-työasemat löytävät muutenkin vain **#PRE**-avainsanalla määritellyt palvelimet.

#-merkki on kommentti. NT:n nimivälimuistissa voi oletusarvon mukaan olla enintään 100 ennalta ladattua nimeä. Jos #PRE-avainsanalla on määritetty useampia nimiä, vain sata ensimmäistä ladataan nimivälimuistiin; loput #PRE-määritykset ohitetaan käynnistyksen yhteydessä, mutta ne ladataan LMHOSTS-tiedostosta, jos dynaaminen nimiselvitys ei onnistu.
LMHOSTS-tiedostoon voi sisällyttää muiden tietokoneiden LMHOSTS-tiedostoja. Tiedosto sisällytetään **#INCLUDE**-lauseella sen sijaan, että se kopioitaisiin kaikkiin tietokoneisiin. Yleisesti käytetty ja keskitetysti hallittu LMHOSTS-tiedosto kannattaa kopioida monistuspalvelulla useampaan palvelimeen, jotta se olisi aina käytettävissä.

Koska suuret Windows NT -toimialueet voivat ulottua useiden IP-aliverkkojen alueelle, reititinverkoissa PDC:t saattavat olla erossa toisistaan (yhteyden tulee säilyä mm. käytettäessä luottosuhteita) tai toimialueen muut työasemat tai palvelimet ovat erossa PDC:stä, LMHOSTS-tiedostossa voidaan **#DOM-avainsanalla** määrittää erikseen NT-toimialueen PDC:n. #DOM-avainsana kirjoitetaan LMHOSTS-tiedoston riville IP-osoitteen ja tietokonenimen jälkeen, minkä jälkeen tulee kaksoispiste ja sen toimialueen nimi, johon PDC kuuluu. Esimerkiksi:

```
193.88.121.65      V1      #DOM:VERSTAS      #toimialueen PDC
```

#DOM-avainsanat lisäävät määrityksiä erityiseen **ryhmänimien välimuistiin**, jolla rajoitetaan paikallisen toimialueen ohjauskoneelle tarkoitettujen sanomien jakelua aliverkkojen välillä. Toimialueelle kuuluvien paikallisten NT-mikrojen LMHOSTS-tiedostoissa on oltava #DOM-määritys kaikille niille saman toimialueen NT-palvelimille, jotka sijaitsevat **muissa aliverkoissa**. Usein käytetylle toimialueen ohjauskoneelle kannattaa lisätä #DOM-määrityksen jälkeen #PRE-avainsana.

Toimialueen varaohjauskoneina eli varapalvelimina (*Backup Domain Controller*) toimivien palvelimien LMHOSTS-tiedostoissa on oltava toimialueen pääohjauskoneen (*Primary Domain Controller*) nimi ja IP-osoite sekä määritykset kaikille muille varaohjauskoneille, jotta jonkin palvelimen muuttuminen toimialueen ohjauskoneeksi ei vaikuta palvelujen tarjoamiseen. Jos toimialueiden välillä on luottosuhteita, voidaan LMHOSTS-tiedostolla mukavasti määritellä, minkä palvelimien välillä luottosuhdetta ylläpidetään.

Paikalliselta toimialueelta selattavia muita toimialueita varten LMHOSTS-tiedostossa on oltava vähintään etätoimialueen pääohjauskoneen eli pääpalvelimen (PDC) nimi ja IP-osoite. On myös hyvä lisätä tiedostoon varaohjauskoneiden määritykset, jotta varaohjauskoneen muuttuminen pääohjauskoneeksi ei vaikuttaisi etätoimialueen selaamiseen.

Alle 20 toimialueen verkoissa kaikille työasemille ja palvelimille yleensä riittää yksi yhteinen LMHOSTS-tiedosto. Tällöin järjestelmien tulisi käyttää NT:n **monistuspalvelua** (*replikointi*) LMHOSTS-tiedoston jakeluun.

Komennolla **NBTSTAT** voi muuttaa välimuistiin ladattuja määrityksiä, esimerkiksi korjata väärinkirjoitettuja nimiä tai poistaa yleislähetyksellä selvitettyjä nimiä. Nimivälimuistin voi alustaa uudelleen komennolla **NBTSTAT -R,** joka tyhjentää välimuistin, lukee LMHOSTS-tiedoston ja lataa #PRE-määritykset uudelleen välimuistiin.

Vinkkejä:

- Keskitä LMHOSTS-tiedoston ylläpito
- Kommentoi muutokset ja "versionumero" tai päiväys
- Kommenttirivit pidentävät kuitenkin hakuaikoja, sillä jokainen tiedoston rivi käsitellään erikseen
- Pidä LMHOSTS-tiedosto ajan tasalla
- Varmista päivityksen onnistuminen *myös NT-palvelimen käynnistymisen jälkeen*
- Päivitä tiedostoa aina, kun verkkoon lisätään tai siitä poistetaan palvelin
- Luettele tietokoneet tärkeysjärjestyksessä, sillä tiedostoa luetaan rivi kerrallaan alusta alkaen - jos useimmin käytetyt tietokoneet ovat heti tiedoston alussa, ne löytyvät nopeammin

- Lataa usein tarvittavat määritykset mikron nimivälimuistiin #PRE-avainsanalla

- Sijoita #PRE-avainsanalla määritetyt rivit tiedoston loppuun, koska ne ladataan nimivälimuistiin käynnistyksen yhteydessä (*jos ladataan*) eikä niitä tarvita sen jälkeen. Kaikki PDC:t ja tärkeimmät BDC:t kannattaa luetella.

DHCP

DHCP (*Domain Host Configuration Protocol*) on NT-palvelimen palvelu, jonka avulla voidaan dynaamisesti jakaa ja hallita verkossa käytettäviä IP-osoitteita ja -asetuksia. DHCP-työasema voi käyttää mm. seuraavia DHCP-asetuksia:

- Oletusyhdyskäytävä (Default Gateway)

- WINS-palvelin

- DNS-palvelin

Työasemassa konfiguroitavat asetukset voidaan viedä DHCP-palvelimelle.

Näin voidaan välittää työasemalle TCP/IP-asetuksia, jotka muuten jouduttaisiin määrittelemään käsin aina kyseisessä työasemassa. Esimerkiksi **kannettava mikro** (*Lap Top*) voi liittyä paikalliseen verkkoon vaikkapa telakointiaseman (*Docking Station*) tai PCMCIA-verkkokortin avulla. Jos työasema käyttää DHCP:tä, kyseisen verkon DHCP-palvelin antaa työasemalle heti valmiiksi konfiguroidun osoitteen reitittimineen, DNS-palvelimineen jne. ja työskentely työasemalla paikallisen verkon asetuksilla voidaan heti aloittaa.

DHCP-palveluun liittyviä seikkoja:

- Jos käytetään useita DHCP-palvelimia, niiden tulisi jakaa eri osoitealueita. Jos DHCP-palvelin jakaa osoitteita useisiin aliverkkoihin, reitittimessä pitää olla **RFC 1542**- sekä **BOOTP Relay Agent**-tuki. Muuten jokaisessa DHCP-asiakkaita sisältävässä aliverkossa pitää olla oma DHCP-palvelimensa.

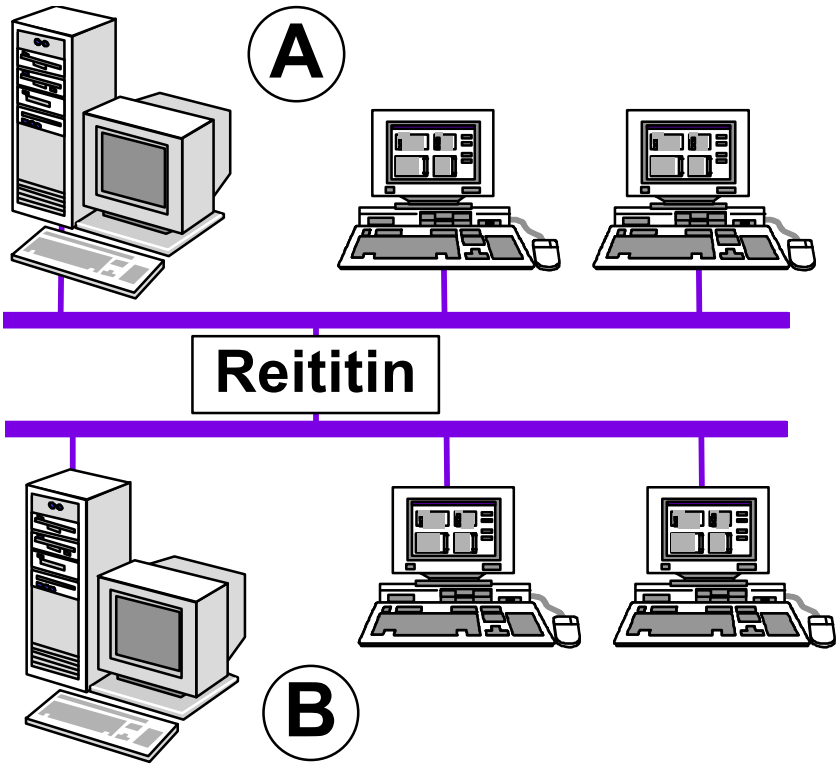
- DHCP-palvelimet eivät kommunikoi keskenään, siispä jokaisen DHCP-palvelimen tulee jakaa omaa osoitesarjaansa.

- MS suosittaa, että DHCP-palvelimet jakaisivat vähintään 75% käytettävissä olevista aliverkon osoitteista ja että reitittimen takana oleva DHCP-palvelin jakaisi samasta vastaavasta aliverkosta 25%.

- Jos DHCP ei toimi reitittimen yli, kokeile liikenteen sallimista **UDP**-porttien **67** ja **68** kautta.

	Verkko A	**Verkko B**
Jaettavat osoitteet aliverkolle A	131.107.4.20- 131.107.4.150	131.107.4.151- 131.107.4.200
Jaettavat osoitteet aliverkolle B	131.107.3.151- 131.107.3.200	131.107.3.20- 131.107.3.150

Esimerkissä on ollut ajatus käyttää aliverkon osoitteista ensimmäisiä osoitteita palvelimille tms kiinteille osoitteille.



Kun DHCP-osoitepyyntö tulee DHCP-palvelimelle, se saa samalla tiedon, mistä aliverkosta pyyntö tuli ja palauttaa aliverkon mukaisen IP-osoitteen.

DHCP otetaan Windows NT 4.0-palvelimessa käyttöön Ohjauspaneelin Network-kuvakkeessa paimalla **Services**-välilehdessä **Add** ja lisäämällä **Microsoft DHCP Server**in.

Ohjeita:

- Voit hallita DHCP-palvelua **DHCP Manager**-valvontaohjelmalla joko paikallisesti palvelimessa tai Windows 95/Windows NT 4.0-työasemasta, johon olet asentanut palvelimien valvontaohjelmat

- Kannattaa vaikkapa tehdä pikakuvake **DHCPADMN.EXE**-ohjelmalle, se löytyy **Winnt\System32**-kansiosta

- Halutun palvelimen voit valita kohteeksi valinnalla **Add | Server**. Anna palvelimen NetBIOS-nimi tai IP-osoite. Voit myös valvoa toista DHCP-palvelinta toisesta DHCP-palvelimesta

- Tarkkaile DHCP-palvelimen tapahtumalokia

- Asentamisen jälkeen jaettava osoitealue perustetaan helpoimmin valitsemalla **Scope | Create**. Anna halutut asetukset (alku- ja loppuosoite sekä mahdollisesti tältä väliltä jakamattomat osoitteet), määrittele varaukset jaetuille osoitteille ja anna nimi ja kuvaus osoitealueelle. Aktivoi tarvittaessa osoitealue valitsemalla **Scope | Activate** tai pysäytä valitsemalla **Scope | Deactivate**

- **DHCP Options**-valikolla määritellään yleiset DHCP-asetukset kaikille jaettaville osoitealueille, valitulle osoitealueelle sekä oletusarvot, jotka tulevat edellisille osoiteryhmille. Asetukset valitulle osoitealueelle saadaan valinnalla **DHCP Options | Scope**

- Valinnalla **DHCP Options** | **Active Leases** nähdään DHCP-palvelimen jakamia osoitteita käyttävät työasemat tai palvelimet. DHCP ilmoittaa myös WINS:ille, jos jonkin työaseman tai palvelimen osoite muuttuu. Kaksoisnapauttamalla työaseman tai palvelimen päälle saadaan yksityiskohtaisemmat tiedot, voit myös varata pysyvästi tietylle Ethernet-osoitteelle halutun osoitteen.

Osoitesarjan luominen ja jakaminen

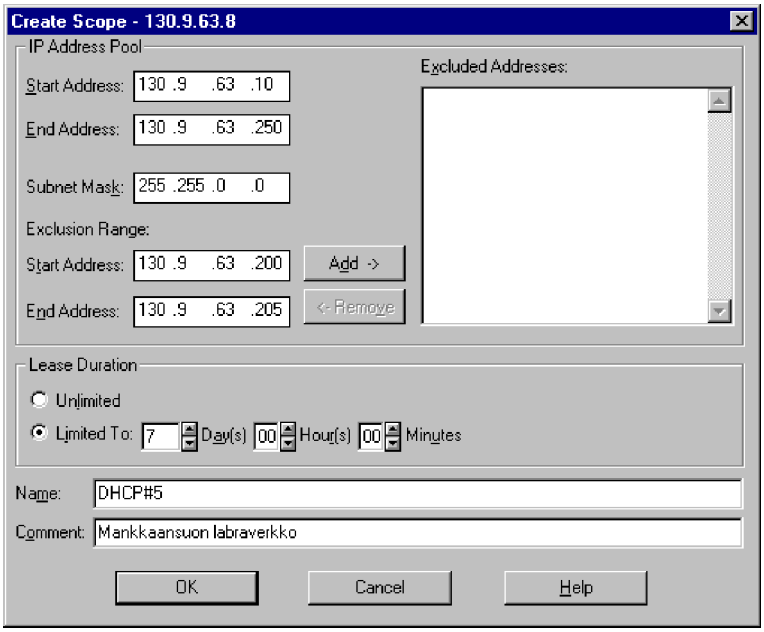
Osoitesarjan luominen ja jakaminen tehdään seuraavasti:

1) Käynnistä **DHCP Manager** ja valitse **Scope** | **Create**

2) Anna seuraavat asetukset:

- **IP Address Pool Start Address** - alkuosoite
- **IP Address Pool Stop Address** - päättymisosoite
- **Subnet Mask** - aliverkon peitto
- **Exclusion Range Start Address** - poissuljettavan osoitealueen alkuosoite
- **Exclusion Range End Address -** poissuljettavan osoitealueen loppuosoite. Paina **Add**-painiketta lisääksesi alueen
- **Lease Duration Unlimited -** osoite varataan työasemalle ikuisesti
- **Lease Duration Limited to** - osoitteen varauksen kesto
- **Name** - nimi
- **Comment** - kommentti

3) Valitse **OK**



4) Valitse **Yes** aktivoidaksesi alueen.

Myöhemmin voit muuttaa asetuksia kaksoisnapauttamalla jaettavan osoitealueen päälle tai valitsemalla alueen ja **Scope** | **Properties**. Voit poistaa aktivoinnin valitsemalla **Scope** | **Deactive** ja poistaa osoitealueen valitsemalla **Scope** | **Delete**.

Osoitesarjan asetukset

Seuraavat ovat asetettavissa DHCP-palvelussa (perässä asetuksen numero):

- Subnet Mask (1)
- Default Router (3)
- DNS Server (6)
- DNS Domain Name (15)
- WINS Server (NetBIOS Name Server) (44)
- NetBIOS Node Type (46)
- NetBIOS Scope Id (47)

DHCP:n asetukset voivat olla seuraavanlaisia (**DHCP Options**):

- **Global -** asetus on voimassa kaikissa DHCP-asiakkaissa, esimerkiksi sama WINS-palvelin
- **Scope** - asetus on voimassa vain tietyssä jaetussa osoitealueessa
- **Default** - oletusasetukset DHCP-asiakkaille.

Asetuksen asettaminen jaetussa osoitealueessa tehdään seuraavasti:

1) Valitse jaettu osoitealue

2) Valitse **DHCP Options** | **Scope**

3) Vaikka asetuksia onkin paljon tarjolla, Microsoft DHCP-asiakkaat voivat käyttää tavallisesti vain seuraavia:

003 Router - reititin; jos asetettu työasemassa, sen asetus ohittaa tämän

006 DNS Server - DNS-palvelin

015 Domain name - DNS-toimialueen nimi

046 WINS/NBT node type -*NetBIOS over TCP/IP*-solmun tyyppi:
1 = B-node (*broadcast*)
2 = P-node (*point-to-point*)
4 = M-node (*mixed*)
8 = H-node (*hybrid*)

044 WINS/NBNS servers - WINS-palvelin; jos asetettu työasemassa, sen asetus ohittaa tämän

047 NetBIOS Scope ID - *NetBIOS over TCP/IP* keskustelee saman Scope ID:n omaavien koneiden kanssa **- älä käytä ilman perusteltua syytä**.

Reititin lisätään seuraavasti:

- Valitse **003 Router**, paina **Add** ja **Value**
- Paina **Edit Array**. Anna IP-osoite kohtaan **New IP Address** ja paina **Add**. Voit myös kokeilla osoitteen selvittämistä antamalla nimen **Server Name** -ruutuun ja painamalla **Resolve**
- Paina lopuksi **OK**. Jos haluat palata **DHCP Manageriin**, paina vielä kerran **OK**

Solmun tyyppi lisätään seuraavasti:

- **046 WINS/NBT node type eli** *NetBIOS over TCP/IP*-solmun tyyppi annetaan alitsemalla **046 WINS/NBT node type**, paina **Add** ja **Value**

- Anna 2 = P-node (*point-to-point*), 4 = M-node (*mixed*) tai 8 = H-node (*hybrid*). Nämä määrittävät miten nimiselvitys tehdään. **B-node** käyttäisi ensin yleislähetystä (*broadcast*) ja sitten annettua nimiselvitysmenetelmää, esimerkiksi WINS tai DNS. **P-node** lähettää kyselyn suoraan WINS-palvelimelle - tämä mm. vähentää verkon kuormitusta. **M-node** käyttää ensin B-nodea ja sitten P-nodea. **H-node** käyttää ensin P-nodea ja sitten B-nodea, ja on suositeltavin ratkaisu.

- Paina lopuksi **OK**

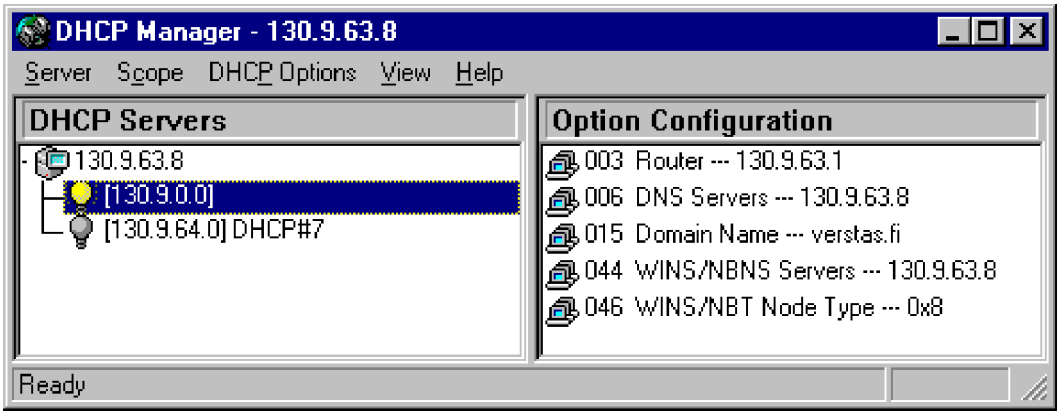
WINS-palvelin:

- Valitse **044 WINS/NBNS servers**, paina **Add** ja **Value** sekä **Edit Array**

- Jälleen voit ehkä ratkaista osoitteen antamalla **Server Name** -kohtaan palvelimen nimen ja painamalla **Resolve**. Paina lopuksi **Add** ja **OK**.

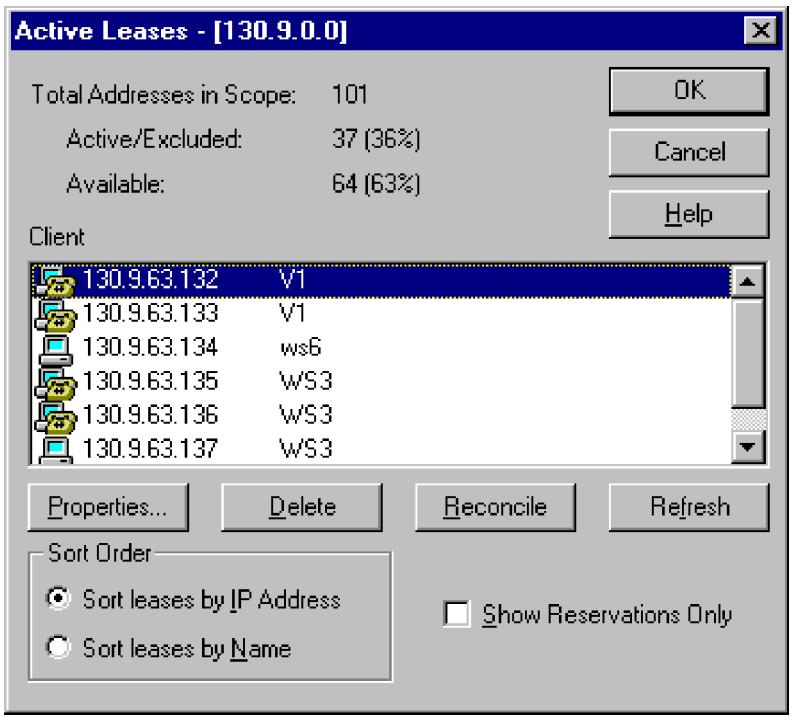
- Määrittele tarvittaessa **047 NetBIOS Scope ID**. Paina lopuksi **OK**.

4) **DHCP Manager** saattaa näyttää esimerkiksi tällaiselta:

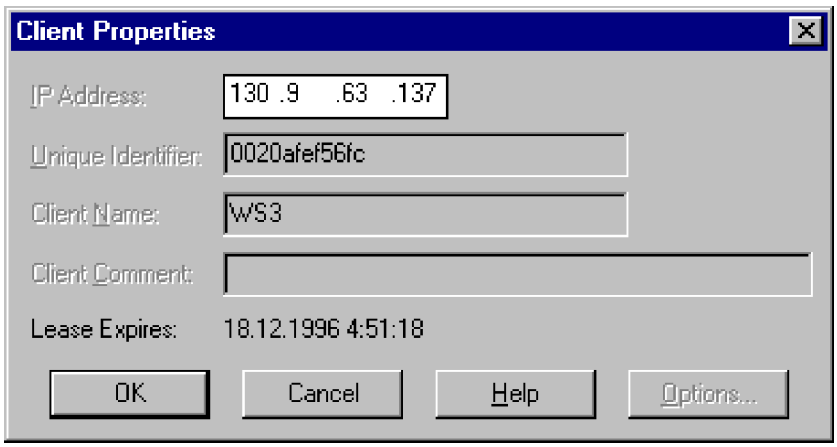


Osoitteiden käyttö

Käytetyt varatut osoitteet näet valitsemalla **Scope** | **Active Leases**:



Tietoja varauksesta saat kaksoisnapauttamalla osoitteen päälle:

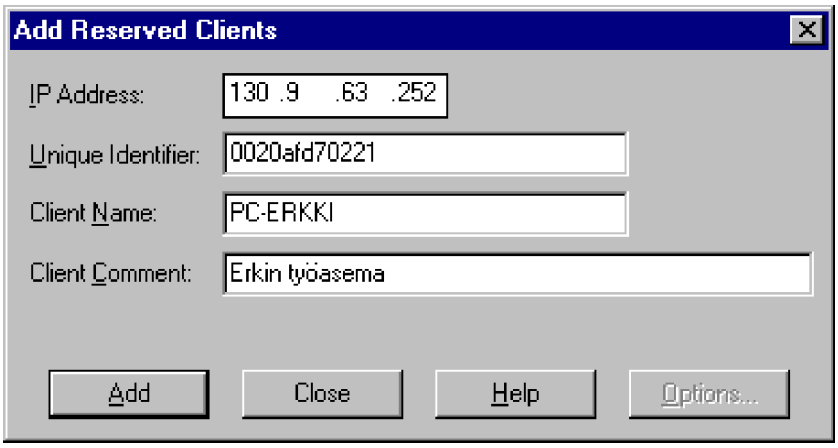


Tällöin näet mm. verkkokortin osoitteen ja varauksen päättymisajan. Jos valitset **Show Reservation Only**, näet vain varatut osoitteet. Painikkeella **Delete** poistettaisiin varaus ja **Reconcile** tarkistaa osoitteiden paikkansapitävyyden DHCP:n tietokannasta.

Osoitteen varaaminen

Voit varata tietyn IP-osoitteen pysyvästi tietylle verkko-osoitteelle. Se tehdään seuraavasti:

1) Valitse **Scope** | **Add Reservations**



2) Anna seuraavat asetukset:

- **IP Address** - varattava osoite
- **Unique Identifier** -verkkokortin yksilöllinen 12 merkkiä pitkä osoite; tämän saa selville työasemassa esimerkiksi komennoilla **NET CONFIG RDR**, **NET CONFIG WKSTA** tai **IPCONFIG /ALL** tai verkkokortin diagnostiikkaohjelmalla
- **Client Name** - työaseman nimi
- **Client Comment** - kommentti

3) Paina lopuksi **Add**.

Tietokannan varmistaminen

DHCP-palvelin käyttää seuraavia tiedostoja **SYSTEM32\DHCP**-hakemistossa:

DHCP.MDB	DHCP-tietokanta
DHCP.TMP	Väliaikainen tietokanta DHCP:n käytön aikana
JET.LOG ja **JET*.LOG**	Tapahtumatietokanta
SYSTEM.MDB	Tietokannan rakennetiedot

JETPACK-apuohjelmalla voit tiivistää tietokannan. Suositus on pienessä verkossa kerran kuukaudessa, isossa kerran viikossa seuraavasti:

1) Pysäytä DHCP-palvelu esimerkiksi komennolla **NET STOP DHCPSERVER**

2) Siirry hakemistoon **SYSTEM32\DHCP** ja anna komento **JETPACK DHCP.MDB TEMPPI.MDB** (nimi **TEMPPI.MDB** viittaa mihin tahansa väliaikaistiedostoon - DHCP.MDB tiivistetään tähän tiedostoon ja se palautetaan DHCP.MDB:ksi ja lopuksi väliaikainen tiedosto poistetaan)

3) Anna komento **NET START DHCPSERVER**

DHCP:n käyttöönotto työasemassa

DHCP otetaan työasemassa käyttöön valitsemalla työasemassa **Hae IP-osoite DHCP-palvelimelta** (Obtain an IP address from a DHCP server) tai valitsemalla **Käytä DHCP:tä** (Enable DHCP).

Jos saat ilmoituksen tyhjästä WINS-palvelimen osoitteesta, älä huolestu; jos verkossa on WINS-palvelin, voit konfiguroida sen osoitteen DHCP-palvelussa **WINS Server (NetBIOS Name Server) (44)**.

Jos määrittelet työasemaan oletusyhdyskäytävän (Default Gateway) ja/tai WINS-palvelimet, nämä asetukset ohittavat DHCP-palvelussa määritellyt asetukset.

Työaseman asetukset näet komennolla **IPCONFIG /ALL**. Työasema voi tarvittaessa uusia osoitteensa seuraavasti:

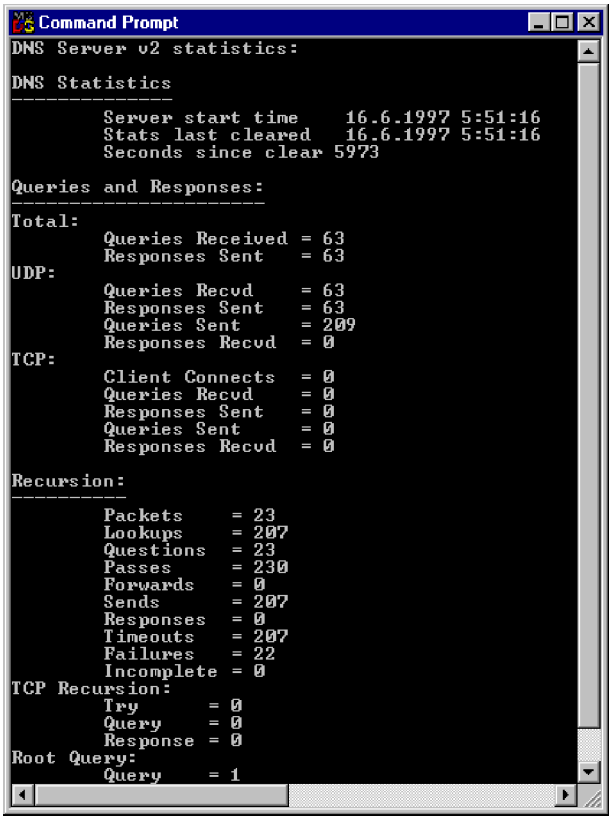
- Komennolla **IPCONFIG /RELEASE** vapautetaan osoite
- Komennolla **IPCONFIG /RENEW** uusitaan osoite

TCP/IP-apuohjelmia

Windows NT 4.0 Resource Kitin mukana tulee myös joitakin hyödyllisiä TCP/IP-apuohjelmia. Windows NT:n TCP/IP-apuohjelmia on käsitelty **Windows NT 4.0 Tehokäyttäjän Opas Osa 1**:ssä.

DNSSTAT

DNSSTAT-apuohjelmalla voidaan seurata DNS-nimipalvelimen statistiikkaa.



Valitsimella **/C** voidaan tilastot tyhjentää.

DHCPCMD

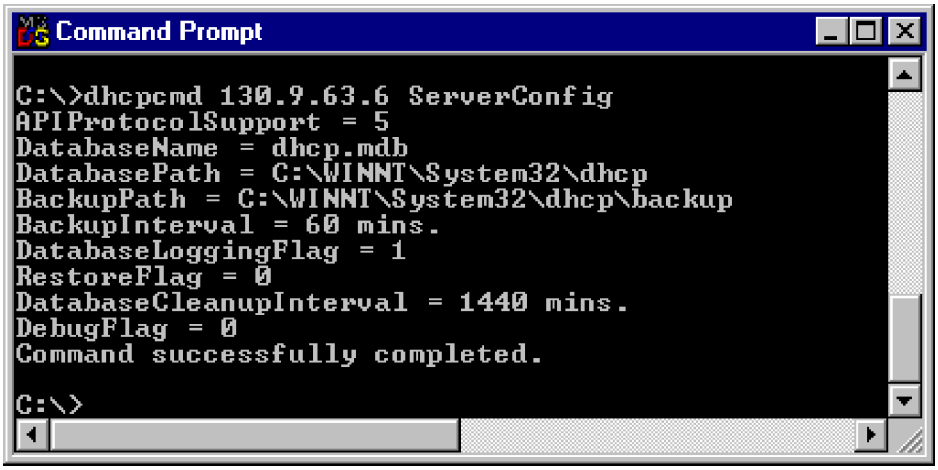
DHCP-palvelimen asetuksia voidaan sekä tutkia että määritellä DHCPCMD-ohjelmalla.

Syntaksi on:

DHCPCMD IP-OSOITE KOMENTO

Komennot ovat:

AddIpRange - alueen lisääminen
AddReservedIp - varatun osoitteenlisääminen
EnumClients - asiakkaiden kysely
ServerConfig - konfiguraatiotiedot
GetVersion - versiotiedot



WINSCHK

WINSCHK on tarkoitettu WINS-tietokannan tarkistamiseen sekä replikoinnin seuraamiseen.

WINSCL

WINSCL on tarkoitettu WINS:in hallintaan; mm. tietokannan eheyden tarkistaminen on mahdollista.

9. INTERNET-PALVELUT

WWW-palvelimet ovat ehkä monipuolisin ja varmasti ainakin laajin koskaan luotu julkaisualusta. Niiden avulla voidaan tuottaa suurelle ja vaihtelevalle yleisölle tekstiä, grafiikkaa, ääntä ja videota ja lisäksi tietoja voidaan päivittää milloin tahansa edullisesti.

Windows NT 4.0-palvelimen mukana tulee **Internet Information Server 2.0**. Sen voi päivittää ilmaiseksi versioon **3.0**. Keskeiset ominaisuudet ovat:

- Integroidut WWW-, FTP- ja Gopher-palvelimet
- Integroitu hallintaohjelma, myös selainpohjainen hallintaohjelma
- Erikseen saatavissa olevia laajennuksia, kuten tietokantatuki, indeksipalvelin jne.

IIS:n lisäksi Windows NT:ssä on muutenkin Internet-käyttöä tukevia toimintoja:

- Windows NT tukee TCP/IP-protokollan ohella modeemin kautta tapahtuvaa yhteydenmuodostusta hyödyntäen **SLIP** (*Serial Line Internet Protocol*)-, **PPP** (*Point-to-Point-Protocol*)- ja **PPTP** (*Point-to-Point-Tunneling Protocol*) -protokollia. TCP/IP:ssä voidaan hyödyntää Windows NT-palvelimen **DHCP** (*Domain Host Configuration Protocol*)-protokollaa ja nimipalveluissa **DNS**- ja **WINS**-tukea
- Windows NT:n mukana tulevat **FTP**- ja **Telnet**-ohjelmat sekä **Internet Explorer** WWW-selain.

Lisäksi on Microsoftilta on saatavissa **Microsoft Proxy Server**-välityspalvelin (koodinimi *Catapult*) ja laaja paketti nimeltä **Microsoft Commercial Internet System** (**MCIS**, koodinimi *Normandy*), johon on koottu useita internet-palvelimia (mm. SMTP/POP3-sähköposti). Seuraava versio on nimeltään **Microsoft Site Server**.

Tulossa on lisäksi / on tullut **Microsoft Transaction Server** (*Falcon*) ja **Microsoft Messaging Queue Server** (*Viper*).

WWW-tekniikka

Seuraavaksi katsotaan, miten WWW-palvelimen ja asiakkaan (selaimen) välinen yhteys muodostuu ja miten tiedonsiirto tapahtuu.

Hypertext Markup Language (HTML)

WWW-sivut on koodattu HTML-muodossa (Hypertext Markup Language). HTML-tiedostot ovat yksinkertaisesti ASCII-tekstitiedostoja, joihin on upotettu muotoilu- ja hypertekstilinkkien koodeja. HTML-tiedoston voi luoda milloin tahansa, kunhan vain mikrossa on tekstinkäsittelyohjelma ja käyttäjä tuntee HTML-muotoilukäskyt. HTML-koodin tekemisen automatisoivia ohjelmia on tarjolla valtavasti, halvimmat (ilmaiset) löytyvät internetistä. Kun HTML-tiedostot ja kaikki niihin liittyvä aineisto on valmis, ne sijoitetaan WWW-palvelimelle ja annetaan käyttäjien käyttöön.

Sisältöä (*Content*) suunnittellessa ja tehdessä täytyy muistaa, että sisällön on kehityttävä samaa tahtia WWW-palvelimen pystyttämisen kanssa!

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (**HTTP**) on protokolla, jonka avulla internetin kautta voidaan käsitellä **HTML**:ää (*Hypertext Markup Language*). HTML on kuvauskieli, jolla luodaan WWW-sivuja. HTTP-protokolla eroaa muista internetissä käytettävistä tiedonsiirtoprotokollista (kuten **FTP**:stä, (*File Transfer Protocol*)), siinä että HTML osaa hyperlinkit. HTML tukee asiakirjoissa olevia hypertekstilinkkejä ja siirtyy välittömästi toisille WWW-sivuille, kun niihin johtavat linkit aktivoidaan. Oikeastaan nimitys hyperteksti on nyttemmin harhaanjohtavaa, koska internetissä on muutakin kuin pelkkää tekstiä, mihin HTML oli alun perin tarkoitettu. Parempi termi onkin **hypermedia**, koska se käsittää kaikki multimedian muodot: kuvan ja äänen.

HTTP ohjaa WWW-selaimen ja WWW-palvelimen välistä yhteyttä ja näiden kahden järjestelmän välistä tiedonvaihtoa. HTTP on nopea ja tehokas protokolla, ja se valvoo monia erilaisia asiakkaan ja palvelimen välillä tapahtuvia toimintoja. Protokollan laajennettu versio, **HTTPS** (HTTP-Secure), tarjoaa salakirjoitetun käyttäjätunnistuksen ja **istunnon välityksen** (*Session transmission*) asiakkaan ja palvelimen välillä. HTTP käyttää **TCP**:tä (*Transmission Control Protocol*).

CERNissä työskentelevä **Tim Berners-Lee** teki ehdotuksen alkuperäisistä hypertekstiprotokollista vuonna 1989. Tuolloin tarkoituksena oli, että tutkijat pääsisivät nopeasti käsiksi toisten tutkijoiden töihin. Projekti aloitettiin vuonna 1990. Berners-Lee ehdotti HTML:ää asiakirjojen muotoilun standardisointiin tarkoitetun **SGML**:n (*Standard Generalized Markup Language*) alastandardiksi. HTML:n myötä uutena ominaisuutena tulivat **hypertekstilinkit**. Berners-Leen työryhmä ehdotti myös HTTP-protokollan käyttöä HTML-asiakirjojen käsittelemiseksi. Projektit olivat suhteellisen valmiita vuoteen 1991 mennessä, ja näin syntyi **World Wide Web**. Muutaman seuraavan vuoden kuluessa selaimia (*Browser*) syntyikin runsain mitoin ja määritelmään lisättiin multimedialaajennuksia.

HTTP käyttää **URL** (*Uniform Resource Locator*) -osoitteenmäärittelyä internet-palvelinten ja niillä olevien asiakirjojen paikantamiseen. Jokaisella WWW:ssä olevalla asiakirjalla on oma yksilöllinen osoitteensa, johon sisältyy sen palvelimen nimi, johon asiakirja on tallennettu.

Uniform Resource Locator (URL)

URL (*Uniform Resource Locator*) on osoitekentässä oleva nimi ja hakemistopolku, kun siirryt hyperlinkkien avulla eri WWW-sivuille. Joskus osoite on kirjoitettava käsin, jos sivulle ei pääse siirtymään linkkien avulla joltakin toiselta sivulta. WWW:n URL-osoitteen syntaksi on

"http:" "//"palvelin [":" portti] hakemistopolku

Merkinnät tarkoittavat:

- URL-osoitteen ensimmäinen osa kertoo **resurssin tyypin** - WWW:ssä tyypin tunniste on **http**
- **Kaksoispiste** erottaa protokollan muusta URL-osoitteesta

- **Kaksi kauttaviivaa** osoittavat, että niiden jälkeen tuleva nimi on palvelimen nimi. Jos et käytä kauttaviivoja, voit viitata palvelimen sisäiseen hakemistopolkuun ja tiedostonimeen

- **Palvelimen nimi** on WWW-sivujen verkkoalueen nimi

- **Porttinumero** käytettäessä HTTP:tä on 80, jota selaimet käyttävät oletuksena. Haluttaessa käyttää jotakin tiettyä porttinumeroa, kirjoitetaan kaksoispiste ja porttinumero palvelimen nimen perään

- **Hakemistopolut** ja HTML-tiedostojen nimet ovat valinnaisia. Kun muodostat yhteyden jollekin WWW-palvelimille, näytetään oletusarvoinen sivu eli kotisivu. Merkintä / tarkoittaa järjestelmän juurihakemistoa. Tyypillisesti Windows-järjestelmissä HTML-tiedostojen tunniste on **.htm**, Unix-järjestelmissä tunniste on **.html**.

Kun siirryt WWW-palvelimessa toisille sivuille, hakemistopolku ja URL muuttuvat. Jokainen toiselle sivulle tai toiseen WWW-palvelimeen osoittava linkki vaatii paikan URL-osoitteen.

Yleensä WWW-osoitteissa ei näy mitään erityistä hakemistopolkua tai HTML-tiedoston nimeä. Useimmiten voidaan käyttää pelkkää Internet-toimialueen (*Domain*) nimeä, kun muodostetaan yhteys WWW-palvelimen kotisivulle. WWW-palvelimet näyttävät automaattisesti palvelimen juurihakemiston oletukseksi määritellyn sivun, kun URL-osoitteeksi annetaan vain toimialueen nimi. Kun osoitteessa annetaan jonkin alihakemiston nimi, näytetään sen hakemiston oletukseksi määritelty sivu, jos sellainen on olemassa. Mahdollisuus näyttää kunkin hakemiston oletussivu tarjoaa helpon tavan organisoida informaatiota WWW-palvelimella:

www.w3.org/pub/WWW/Protocols

URL:n vasen osa on verkkoalueen nimi. URL:n hakemistopolku osoittaa **pub/WWW/Protocols**-nimiseen hakemistoon, jossa on WWW:ssä käytettäviä protokollia koskevia dokumentteja. Tässä tapauksessa pääkäyttäjä on järjestänyt hakemistot loogisesti siten, että niiden nimet kertovat, mitä hakemistossa on. Jos hakemistossa ei ole oletustiedostoa, selain saattaa näyttää hakemistolistauksen, mikäli pääkäyttäjä on niin määritellyt.

Useimmiten näin ei kuitenkaan ole tietoturvasyistä, mutta palvelimissa,

joissa on paljon kopioitavaksi tarkoitettuja tiedostoja hakemistolistaus saattaa näkyä.

HTTP-linkkiprosessi

Kun selaimen osoitekenttään kirjoitetaan uuden WWW-palvelimen URL-osoite, nimi on ensiksi muutettava internet-osoitteeksi. Selain tekee pyynnön **DNS-palvelimelle** ja lähettää sen internettiin.

Pyyntö lähetetään käsiteltäväksi lähimmälle DNS-palvelimelle. Jos DNS-palvelin ei tunne osoitetta, se lähettää pyynnön edelleen ylöspäin hierarkiassa. Kun lopulta löytyy DNS-palvelin, joka tuntee osoitteen, IP-osoite lähetetään takaisin selaimelle. Tämän prosessin aikana näytöllä näkyy ilmoitus, joka voi olla vaikkapa *Finding site*.

Nyt selaimella on IP-osoite, jota se voi käyttää palvelimen kanssa. Yhteyspyyntö lähetetään TCP-pakettina, jossa on kohteen IP-osoite sekä lähettäjän IP-osoite (jotta kohdepalvelimen ei tarvitse tehdä samaa DNS-kyselykierrosta uudelleen). Paketti lähetetään internettiin, jossa se kulkee reitittimestä toiseen, kunnes se saapuu kohdepalvelimeen. Kaikki tämä tapahtuu muutamassa sekunnin murto-osassa.

> Pakettien on ehkä kuljettava välityspalvelinten (*Proxy*), yhdyskäytävän (*Gateway*) tai palomuurin (*Firewall*) kautta. Nämä ottavat vastaan pyyntöjä asiakkailta ja joko muotoilevat viestit uudelleen, suodattavat ne pois tietoturvallisuussyistä tai kääntävät viestit.
>
> **Suodattaminen** perustuu IP-osoitteisiin ja pyydetyn palvelun tyyppiin. Jos palomuuri hyväksyy paketin, se lähetetään palvelimelle, joka sitten kääntää sen tarvittavalle prosessille (portille). Joskus saattaa olla, että palvelin tai prosessit ovat varattuja, eivätkä ehdi käsitellä paketteja, koska suositut palvelimet saattavat käsitellä samanaikaisesti tuhansilta asiakkailta tulleita pyyntöjä. Jos paketit hyväksytään, palvelin koostaa palautepaketit, jotka lähetetään takaisin selaimelle.
>
> Yksi välittäjänä toimivien palvelimien mielenkiintoinen piirre on, että ne voivat tallentaa aikaisempien pyyntöjen täyttämiseen käytettyjä tietoja välimuistiin (*Cache*) ja käyttää näitä tietoja muiden asiakkaiden tekemien pyyntöjen täyttämiseen.

Nyt selaimella on yhteys palvelimeen, ja jos URL-osoitteessa on verkko-

alueen lisäksi muita osia, ne käsitellään seuraavaksi. URL-osoite saattaa sisältää hakemistopolun ja tiedostonimen, ja tässä vaiheessa selain lähettää ne pyyntönä palvelimelle. Jos osoitteessa ei ole mainittu mitään erityistä hakemistoa, pyyntö kohdistetaan palvelimen pää- eli juurihakemistoon (*Root Directory*). Tällöin palvelin vastaanottaa pyynnön ja vastaa lähettämällä oletussivun takaisin selaimelle. TCP pakkaa HTML-sivutiedot IP-paketteihin, jotka lähetetään selaimelle.

WWW-palvelimelta tulevat tiedot saattavat sisältää seuraavia:

- Käytettävän HTTP:n version
- Pyynnön tilatiedot, kuten löytyikö tieto vai ei
- MIME-tyypin (Multipurpose Internet Mail Extensions), joka määrittelee mediatyypin (tekstiä, ääntä, kuvia, videota jne.)
- Itse sisällön

Kun palvelin on suorittanut tiedonsiirron loppuun, se sulkee yhteyden. Yhteyttä ei ole tarpeen pitää avoimena, koska toisessa päässä oleva käyttäjä saattaa kuluttaa jonkin aikaa sivun lukemiseen, ennen kuin hän lähettää palvelimelle uuden pyynnön.

Jos käyttäjä napauttaa hiirellään sivulla olevaa hyperlinkkiä, muodostetaan uusi yhteys. Tässä vaiheessa ei enää tarvita uutta DNS-kyselykierrosta, koska oikea IP-osoite on tiedossa ja tallennettuna välimuistiin. Tämä yhteyden muodostaminen ja katkaiseminen on osa HTTP:n tilatonta luonnetta. Koska monet muutkin IP-paketit käyttävät yhteyslinkkejä, palvelimen täytyy antaa yhteysaikaa myös muille käyttäjille. **Yhteyden katkaiseva** tilaton protokolla varmistaa, että linkkejä käytetään tehokkaasti ja pienentää järjestelmän resurssivaatimuksia, koska sen ei tarvitse säilyttää tietoja asiakkaista ja palvelimista.

Näin sekä asiakkaat että palvelimet voivat joustavasti ja nopeasti vaihtaa yhteyksiä, mikä onkin hyperlinkkien ydinajatus.

Yhteyden säilyttävää protokollaa käytettäessä sekä asiakas että palvelin säilyttävät linkin ja sen tiedot muistissa, vaikka tietoa ei siirrettäisikään. Nämä protokollat vaativat järjestelmältä enemmän muistia, jotta ne voivat pitää muistissa suurta määrää asiakkaita. Tämä taas kuormittaa tietoliikenneyhteyksiä. Nämä protokollat ovat käyttökelpoisia liiketoimintatransaktioissa ja valvontatehtävissä. Tällaisten protokollien käyttö kasvanee WWW:n laajetessa.

HTTP-viestit

Asiakkaat ja palvelimet tekevät pyyntöjä ja vastaavat toisilleen käyttäen viestejä. Viestit alkavat, kun asiakas pyytää yhteyttä palvelimeen. TCP pakkaa viestit IP-paketteihin, jotka siirrettään verkon välityksellä. Tässä kuvatut tärkeimmät pakettityypit antavat jonkinlaisen käsityksen siitä, miten HTTP toimii.

Viestit ovat:

- **GET** - hae tietoa URL-osoitteessa määritellyltä palvelimelta. Palvelin vastaa lähettämällä oletusasiakirjan tai pyydetyn asiakirjan. Asiakirjoissa on niiden tekijöiden niihin varta vasten sisällyttämät otsikkotiedot, jotka yksilöivät asiakirjan. Otsikkotiedoissa on otsikko, kuvaus, asiakirjan suhde muihin palvelimen asiakirjoihin ja asiakirjan URL-osoite.

- **HEAD** - tämä viesti on samanlainen kuin GET, mutta tässä palvelin lähettää vain otsikkotiedot, ei varsinaista asiakirjaa. WWW:ssä toimivat hakutietokantoja tekevät hakurobotit käyttävät tätä viestiä halutessaan tietoja WWW-palvelinten asiakirjoista. HEAD-viestiä käytetään myös testattaessa hypertekstilinkkien oikeellisuutta, toimivuutta ja tehtyjen muutosten toimivuutta.

- **POST** - tämä viesti kertoo palvelimelle, että sen pitäisi kommentoida (**annotate**) olemassa olevia resursseja, postittaa viesti (sähköisille ilmoitustauluille, keskusteluryhmiin tai postituslistoille), lähettää lomakkeen tiedot käsiteltäviksi tai lisätä tietoja tietokantaan.

Selaimet ja palvelimet käyttävät yhteydenpidossaan myös muita viestejä. Edellämainitut ovat kuitenkin tärkeimmät, ja niiden avulla pitäisi jo saada jonkinlainen käsitys siitä, kuinka asiakkaat ja palvelimet keskustelevat keskenään. Lisätietoja HTTP:stä ja muista WWW-protokollista löytyy World Wide Web Consortiumin (W3C) WWW-sivuilta osoitteesta **www.w3.org./pub/WWW/Protocols**

S-HTTP (Secure HTTP)

Secure HTTP (S-HTTP) tarjoaa tavan salata asiakkaan ja palvelimen välillä kulkeva tieto. S-HTTP käyttää RSA Data Security Inc.:n kehittämää julkisen avaimen salausmenetelmää. Julkisen avaimen salausmenetelmässä organisaatio kehittää kaksi toisiinsa linkitettyä turva-avainta, joita käytetään transaktioissa. Toinen avaimista on julkinen ja toisen yritys pitää salaisena. Tiedonsalausta haluava käyttäjä salaa tiedot julkisella avaimella, ja organisaatio purkaa salauksen yksityisellä avaimellaan.

HTTP-NG (Next Generation)

HTTP-NG (Next Generation) on HTTP:n seuraava kehitysaste, joka tarjoaa paremman suorituskyvyn ja tuo joitakin uusia piirteitä, jotka tukevat kaupallisia sovelluksia kuten tietoturvaa ja käyttäjätunnistusta. Seuraavassa joitakin muutoksia ja parannuksia:

- Vaikka HTTP muodostaakin joka pyyntöä varten uuden yhteyden, HTTP-NG mahdollistaa monen erilaisen pyynnön lähettämisen yhtä yhteyttä pitkin ja parantaa näin suorituskykyä. Asiakkaan ei tarvitse odottaa palvelimen vastausta ennen uuden pyynnön lähettämistä

- Palvelimet voivat vastata pyyntöihin missä järjestyksessä tahansa ja sekoittaa tietoa monesta kohteesta ja näin lähettää kuvia rinnakkain

- HTTP-NG käyttää kanava-käsitettä, jonka mukaan viestit ja tiedot lähetetään eri yhteyttä pitkin. GETin ja POSTin kaltaiset ohjausviestit lähetetään ohjauskanavaa pitkin, ja objektit (kuten kuvat) lähetään muita kanavia pitkin

- HTTP-NG monikanavarakenteineen tukee paremmin tulevaisuuden suurinopeuksisia verkkoja, kuten ATM:ää, ja uusia multimediamuotoja, kuten videota.

Lisätietoja HTTP-NG:stä löytyy aiemmin mainitun World Wide Web Consortiumin (W3C) WWW-sivuilta.

Internet Information Server

Windows NT 4.0 -palvelimen mukana tulee **Internet Information Server 2.0**. Sen voi päivittää versioon **3.0** joko erillisellä päivitysohjelmalla tai asentamalla ensin **IIS 2.0**:n ja sitten **Service Pack 2**:n tai **Service Pack 3**:n.

Mukana on **WWW** (World Wide Web)-palvelin **HTML** (HyperText Markup Language)-tiedostojen tarjoamiseen **HTTP** (Hypertext Transport Protocol) -protokollalla ja **FTP** (*File Transfer Protocol*) -palvelin tiedostojen siirtoon ja **Gopher**-palvelin tiedostojen valikkopohjaiseen esittämiseen.

FTP (*File Transfer Protocol*)-palvelin mahdollistaa tiedostojen siirron käyttäen TCP/IP-protokollaa. Kun käyttäjät liittyvät FTP-palvelimeen, käyttäjät voidaan asettaa käyttämään NT-käyttäjätunnuksia ja -salasanoja. Kannattaa myös asentaa FTP-palvelimen tiedostojenjako kiintolevylle, jolle on asennettu NTFS-tiedostojärjestelmä; tällöin saadaan myös kansioiden suojaustaso käyttöön.

Käyttöönotto

Käyttöönotto noudattelee seuraavia vaiheita:

- Asenna NT-palvelin ja tarkista asetukset
- Aja IIS:n asennus
- Luo IIS:n sisältö
- Testaa IIS:n toiminta.

Tarkistuslistaa:

- IIS-palvelimessa tulee olla oikein konfiguroitu **TCP/IP** (*Transmission Control Protocol/Internet Protocol*) -protokolla
- Palvelimessa tulisi olla **staattinen** (**ei** DHCP-) IP-osoite
- CD-ROM-aseman käyttömahdollisuus (paikallinen tai verkon yli)
- Riittävästi levytilaa IIS-palvelimelle ja sisällölle (määrittele itse)
- Ei olisi huono ajatus varata omaa NTFS-levyosiotaan **Internet Information Server**in palveluita varten

IIS:n liittäminen Internetiin:

- **Internet-liittymä** ja **IP-osoite** (*Internet Protocol*) Internet-yhteyden tarjoajalta (*Internet Service Provider* (ISP)) sekä tarvittavat verkkokortit, modeemit jne
- **DNS-nimi** (*Domain Name System* (DNS)) IP-osoitteelle - esimerkiksi toimialueen (*Domain*) **fishware.fi** WWW-palvelin voisi olla **www.fishware.fi**. Ei ole pakollinen, mutta tällöin IIS-palvelimeen viitataan vain IP-osoitteella, esimerkiksi **http://123.123.123.123**.

IIS:n liittäminen Intranetiin:

- Verkkokortti ja **LAN** (*Local Area Network*)-liitäntä
- **WINS**- (*Windows Internet Name Service*) tai **DNS** (Domain Name System)-palvelin intranetissa. Ei ole pakollinen, mutta tällöin IIS-palvelimeen viitataan vain IP-osoitteella, esimerkiksi **http://123.123.123.123**. Toinen tapa on isäntätiedostot, DNS:n sijasta **HOSTS** ja WINS:in sijasta **LMHOSTS**
- **WWW-virtuaalipalvelimet** - voi myös rekisteröidä useita nimiä samaan palvelimeen, esimerkiksi **www.fishware.fi** ja **www.penguin.fi**. Tällöin tulee määritellä useampi IP-osoite samaan palvelimeen - se tehdään TCP/IP-asetuksissa valitsemalla **Advanced TCP/IP Configuration**. Voit myös määritellä nämä eri

nimet ja IP-osoitteet nimipalvelussa

Käyttäjätunnukset ja suojaukset:

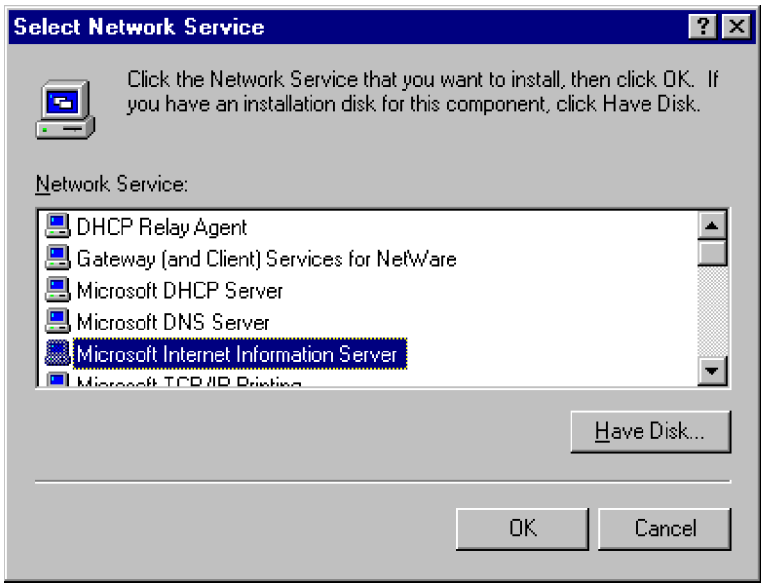
- Tarkista **IUSR_palvelinnimi** -käyttäjätunnuksen oikeudet
- Käytä vaikeasti arvattavia salasanoja ja käytä sekaisin sekä kirjaimia, numeroita että erikoismerkkejä
- Ota käyttöön tiukat suojaukset (ks. **Luku 11**)
- Poista tarpeettomat käyttäjätunnukset **Administrators**-ryhmän jäsenyydestä
- Ota käyttöön NTFS ja valvonta (*Auditing*)
- Aja IIS-palvelimessa vain tarpeellisia palveluita
- Poista tarpeettomat sidokset (*Bindigs*) ja palvelut (*Services*) verkkokorteista
- Tarkista verkkoon jaettujen resurssien käyttöoikeudet.

IIS:n asentaminen

Asentaminen tehdään seuraavasti:

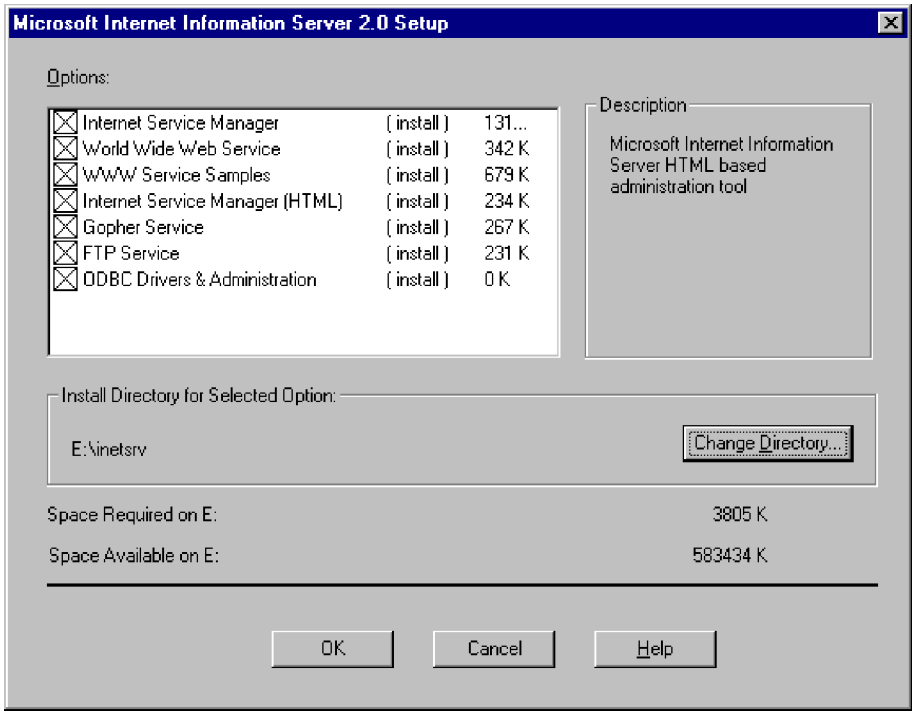
1) Työpöydältä valitsemalla **Install Internet Information Server**

tai Ohjauspaneelista **Networkin** avulla lisäämällä **Network Service**-välilehdessä **Microsoft Internet Information Server**



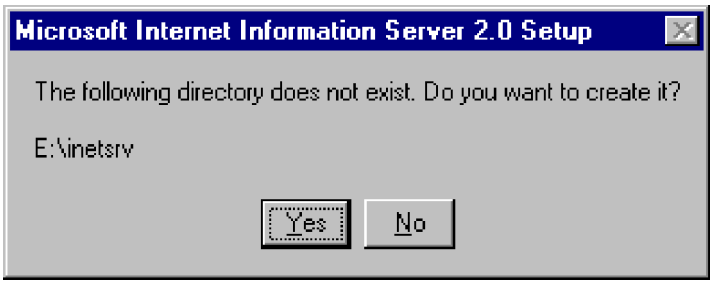
2) Paina **OK**. Asennusohjelma pyytää asentamaan CD-ROM:in asemaansa. Jos palvelimen asennustiedostot on jaettu verkkoon, voit ehkä antaa myös UNC-polun (esimerkiksi **\\P1\ASENNUS\NT40SRV.i386** tms)

3) Voit valita halutut komponentit ja **Change folder**-painikkeella voit muuttaa palvelun käyttämää oletuskansiota. Paina **OK**.

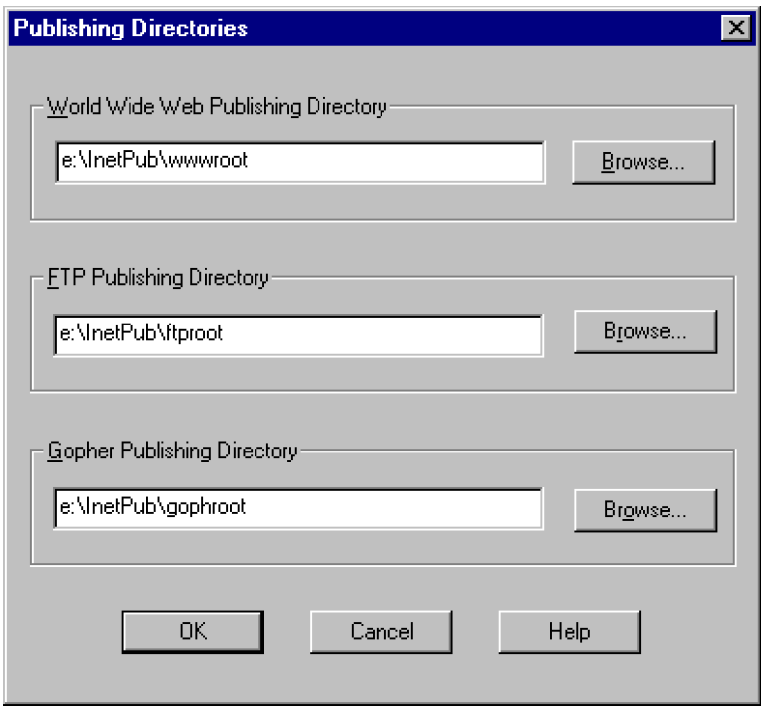


WWW-selaimen kautta käytettävää **Internet Service Manager (HTML)**:ää ei oletuksena asenneta, mutta se on kuitenkin varsin hyödyllinen, koska IIS:n hallinta onnistuu mistä tahansa työasemasta, jossa on selain - eikä se vaadi suunnattomasti levytilaa palvelimelta!

4) Seuraavaksi kysytään palvelimen asennushakemiston luominen, jos sitä ei ole olemassa. Vastaa **Yes**.

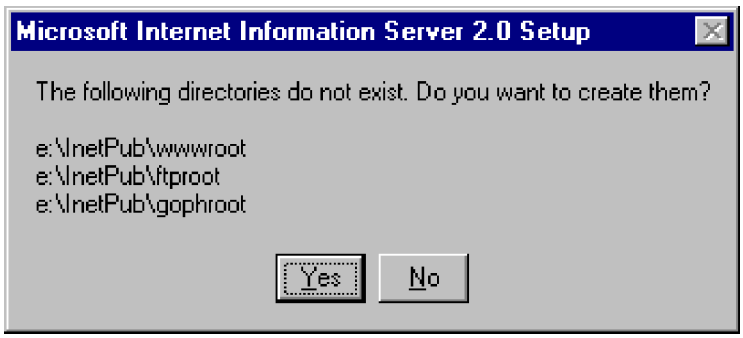


5) Sitten voit valita palvelu- ja kansiokohtaisesti eri palvelujen käyttämät kansiot - ei järjestelmälevylle, vaan omalle levyosiolleen:

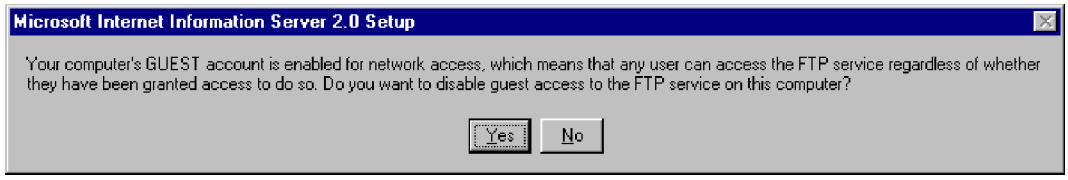


6) Paina **OK**. Jos kansioita ei ole olemassa, ne luodaan.

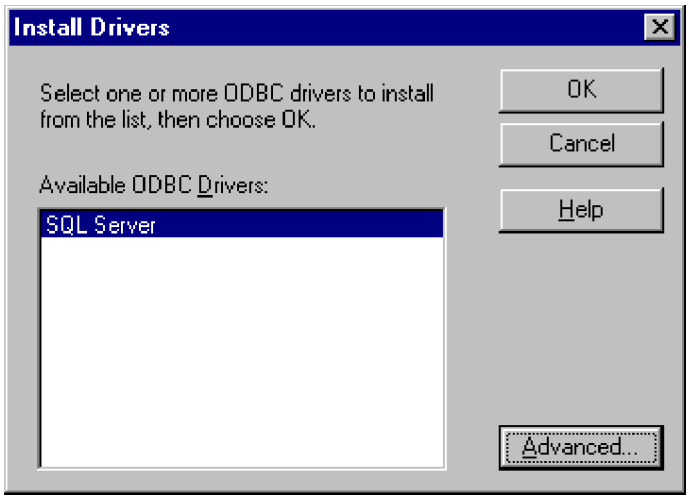
7) Tämän jälkeen kysytään kansioiden luomisesta: vastaa **Yes**:



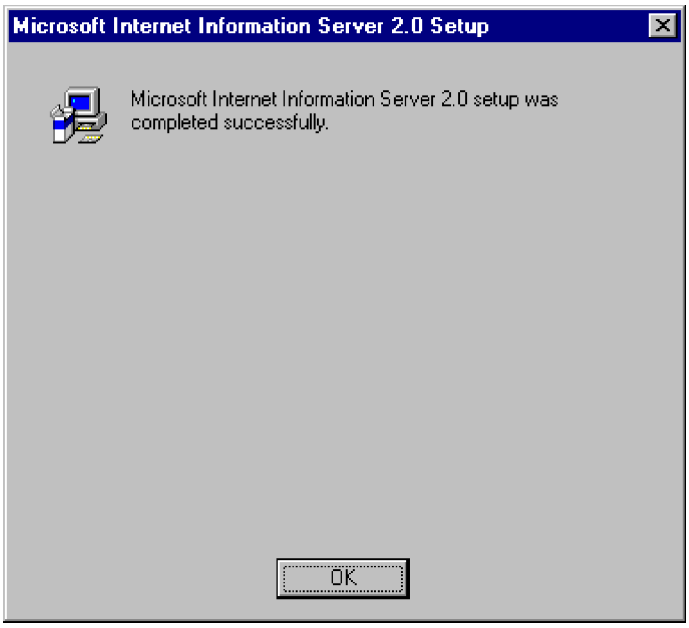
8) Jos **Guest** -käyttäjätunnus pääsee palvelimeen verkon kautta, FTP-palvelimen asennuksessa tarjotaan mahdollisuutta estää Guest-käyttäjän pääsy FTP-palveluun. Valitse **Yes** tehostaaksesi tietoturvallisuutta.



9) Seuraavaksi asennetaan tarvittaessa **ODBC** (*Open DataBase Connectivity*)-ohjaimet. ODBC:n avulla voit liittää WWW-palvelimen esimerkiksi **SQL Serveriin**. Paina **OK**.



10) Lopulta asennus päättyy.



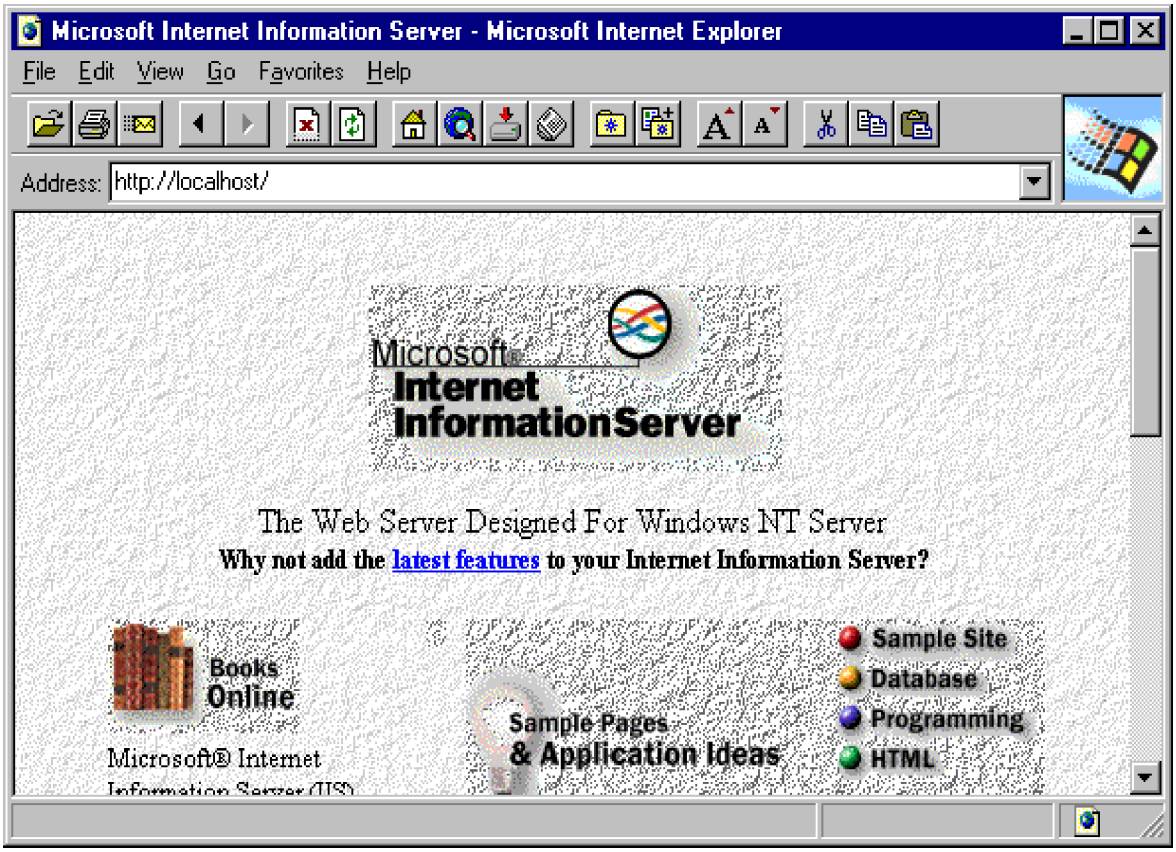
Voit ryhtyä heti testaamaan sekä konfiguroimaan palveluita.

Ei olisi kuitenkaan huono ajatus asentaa NT-palvelimeen uudelleen siinä ollut **Service Pack**, koska asennusohjelma on *saattanut* kirjoittaa joidenkin uudempien DLL:ien päälle.

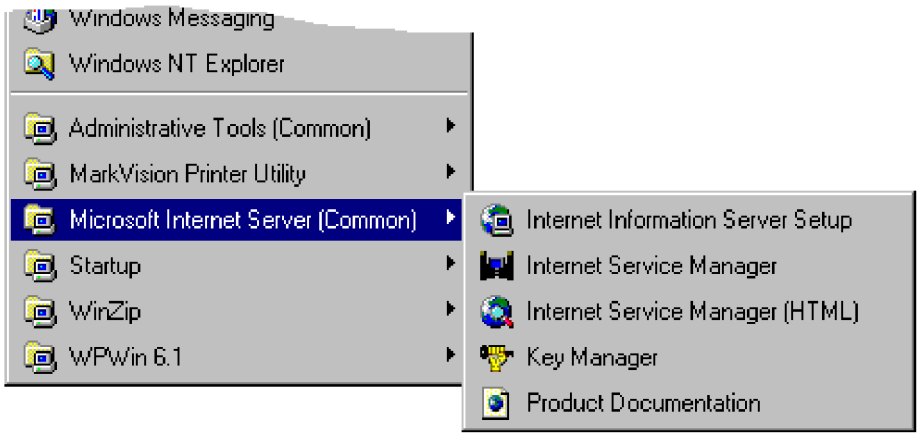
Asennuksen jälkeen **Start**-valikon **Programs**-valikosta löytyy valikko **Microsoft Internet Server**.

Asennusohjelma on myös luonut paikallisen käyttäjätunnuksen **IUSR_(palvelimen nimi)**, joka kuuluu **Guests**-ryhmään ja jota käytetään anonyymeissä yhteyksissä WWW-vertaispalveluihin. Käyttäjätunnuksella on muuten oikeus kirjautua paikallisesti käyttäjäksi (**Log on locally**).

Voit testata WWW-palvelimen toimintaa käynnistämällä **Internet Explorerin** ja antamalla URL-osoitteeksi **Address**-kohtaan palvelimen nimen (NetBIOS-nimi) tai nimen **localhost** - **http://**-alkuliitettä ei tarvitse määritellä:



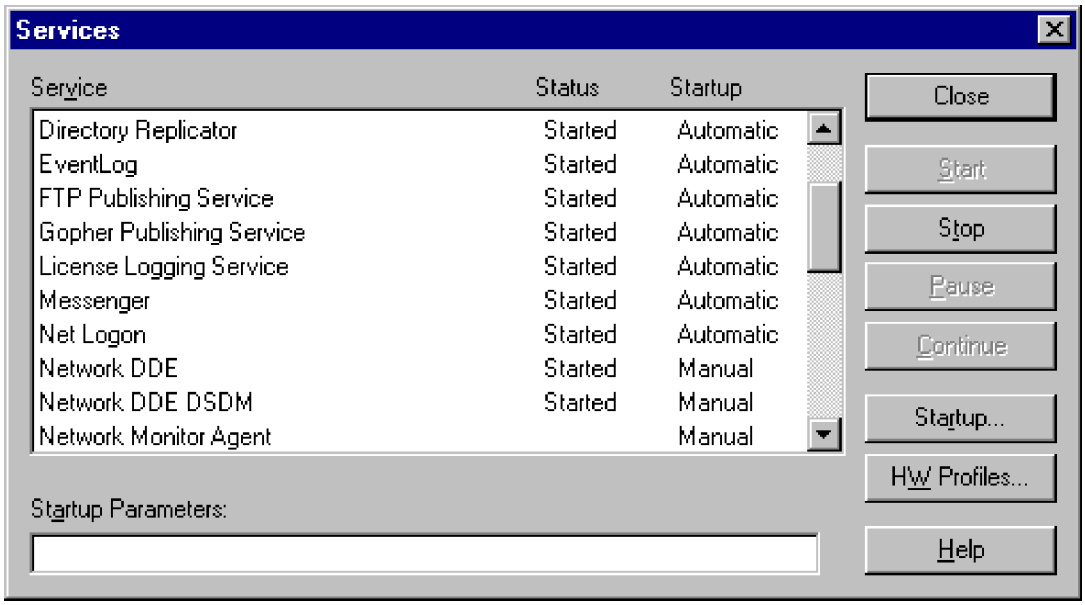
Asennuksen jälkeen **Start**-valikon **Programs**-valikosta löytyy uusi valikko, **Microsoft Internet Server**:



Valinnat ovat seuraavat:

- **Internet Information Server Setup** - asennusohjelma
- **Internet Service Manager** - FTP-, WWW- ja Gopher-palveluiden hallinta
- **Internet Service Manager** (HTML) - selaimella käytettävä FTP-, WWW- ja Gopher-palveluiden hallinta
- **Key Manager** - yksityisen ja julkisen salausavaimen luominen
- **Product Documentation** - kattava opas palvelujen hallinnasta.

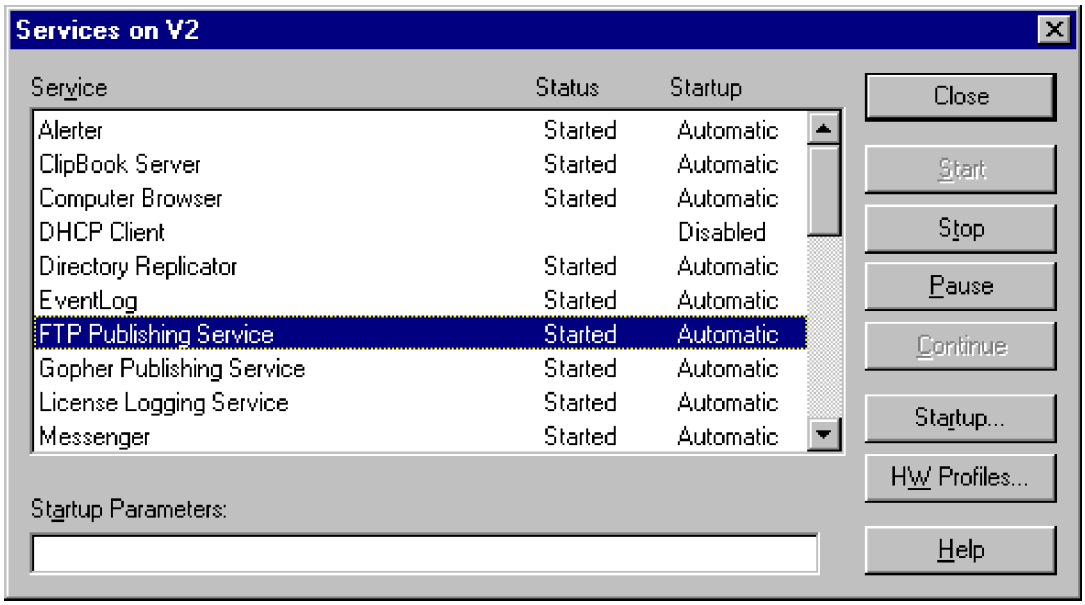
Löydät myös käynnistetyt palvelut Ohjauspaneelin **Services**-kuvakkeella.



Automaattisesti käynnistyvät palvelut ovat:

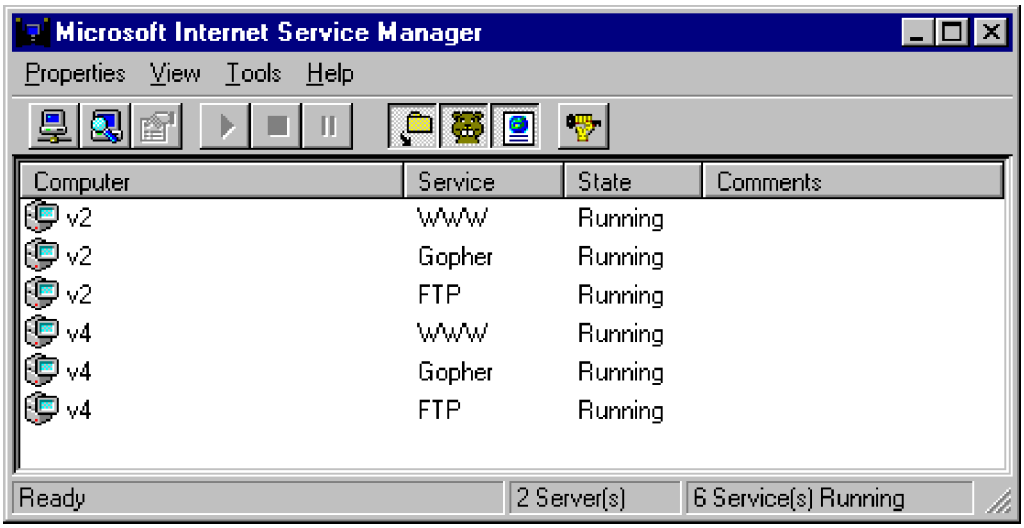
- FTP Publishing Service
- Gopher Publishing Service
- World Wide Web Publishing Service.

Voit lisäksi käyttää tavallisia palveluiden hallintaohjelmia, kuten **Server Manageria**, tai komentorivin komentoja (**NET START**, **NET STOP**):



Internet Service Manager

Internet Service Manager -ohjelmalla voit hallita FTP-, WWW- ja Gopher-palveluja.



Hallinnassa käytettävät valikot ovat:

- **Properties** - voit kytkeytyä eri palvelimiin (myös IIS-palvelimiin) ja hallita niiden palveluita
- **View** - voit valita halutun näkymän palvelimiin ja palveluihin.

Valitse haluttu palvelu. Ominaisuudet näet seuraavilla tavoilla:

- Paina **Enter**
- Kaksoisnapauta palvelua
- Valitse **Properties** | **Service Properties**.

Jos asensit **Internet Service Manager (HTML)** -ohjelman, niin voit hallita FTP-, WWW- ja Gopher-palveluja myös selaimen kautta. Ainoa, mitä **et** voi tehdä, on palveluiden pysäyttäminen.

Esimerkissä on käytetty paikallisen tietokoneen **localhost** -tunnusta

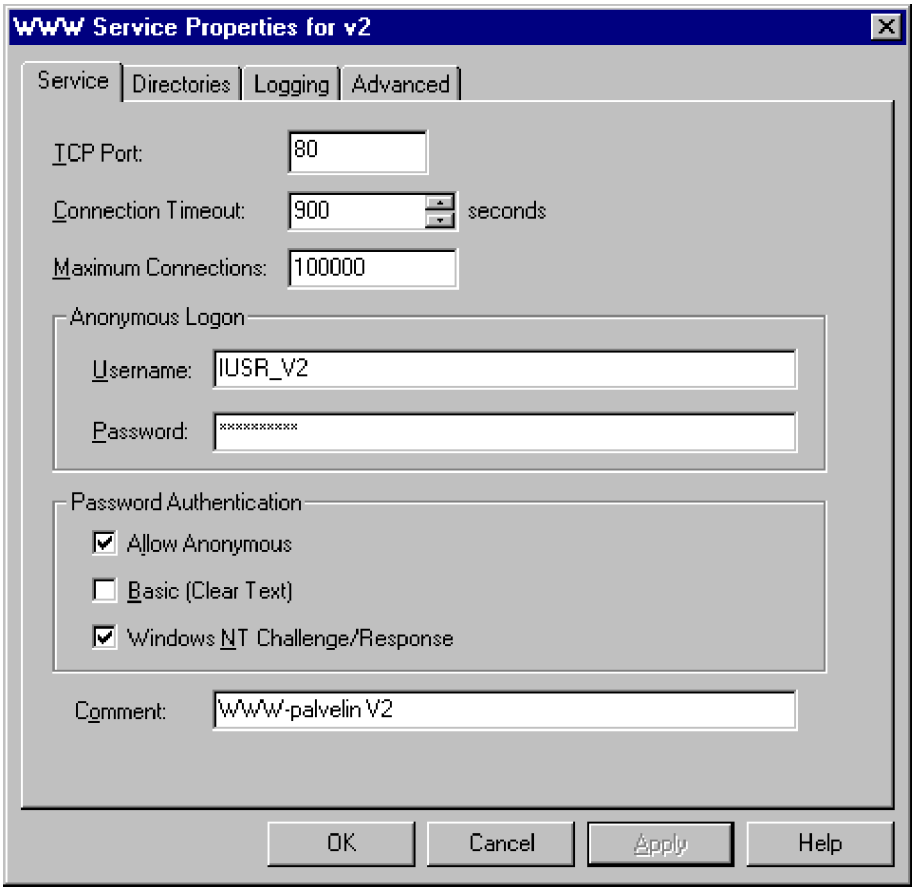
(127.0.0.1).

WWW-palvelimen asetukset

WWW-palvelimen asetuksissa on neljä välilehteä:

- **Service** - palvelu
- **Directories** - kansio
- **Logging** - loki
- **Advanced** - lisäasetukset.

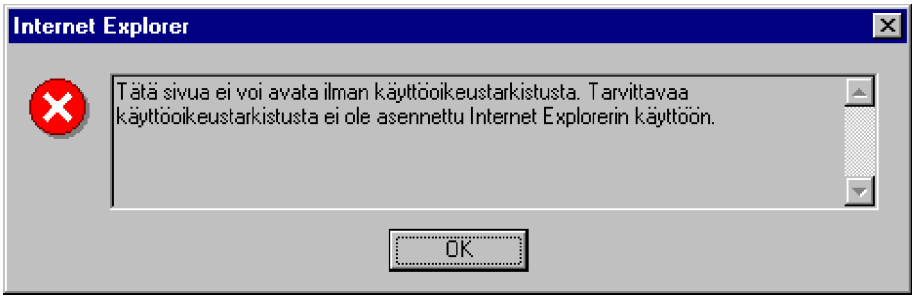
Service



Service-välilehdessä voit asettaa seuraavat:

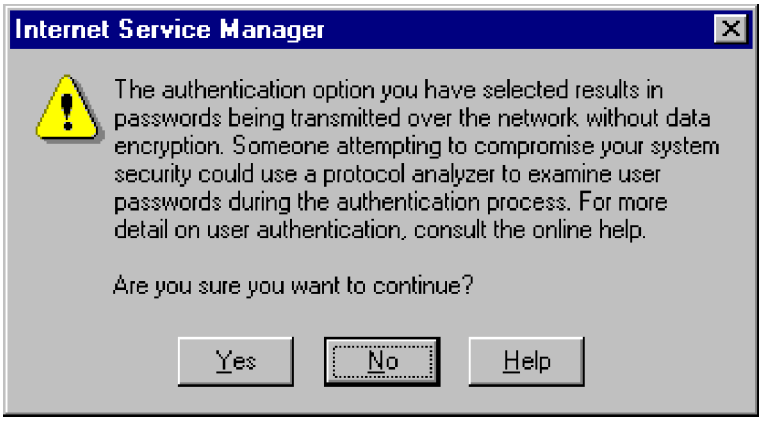
- **TCP Port** - palvelimen käyttämän portin numero, oletus **80**
- **Connection Timeout** määrittelee yhteyden aikakatkaisun, jos käyttäjä ei tee mitään annetun ajan kuluessa
- **Maximum Connections** - samanaikaisten käyttäjien maksimimäärä
- **Anonymous Logon** - jos käyttäjä ei anna käyttäjätunnustaan, oletuksena käytetään paikallista käyttäjätunnusta **IUSR_(palvelimen nimi)**, mikä on annettu **Username**-kohdassa ja **Password** on myös määritelty
- **Password Authentication** - salasanan tarkistus:
  - **Allow Anonymous** - määrittelee, vaaditaanko käyttäjiä kirjautumaan käyttäjätunnuksella käyttäjäksi vai sallitaanko nimettömät kirjautumiset.

Jos et ole määritellyt lisäksi jompaa kumpaa käyttöoikeustarkistusta, saatat törmätä ongelmiin käyttöoikeustarkistuksen kanssa:

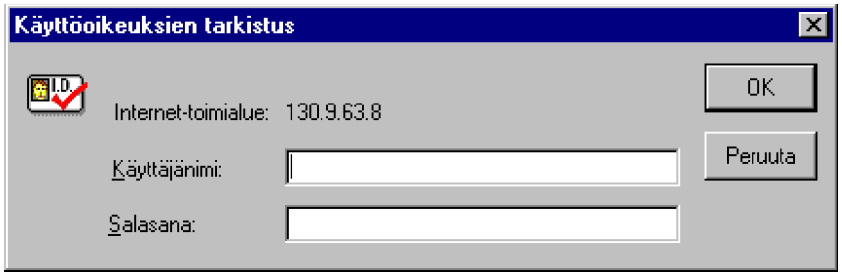


Lisäksi pitää määritellä seuraavat menetelmät:

- **Basic (Clear Text)** on yleensä kaikkien selaajien tukema menetelmä kysyä käyttäjätunnukset ja salasanat. Ne lähetetään salakirjoittamattomina, josta tuodaan näyttöön huomautus:



Miltä käyttöoikeustarkistus näyttää, riippuu selaajasta. Internet Explorerissa se näyttää tältä:

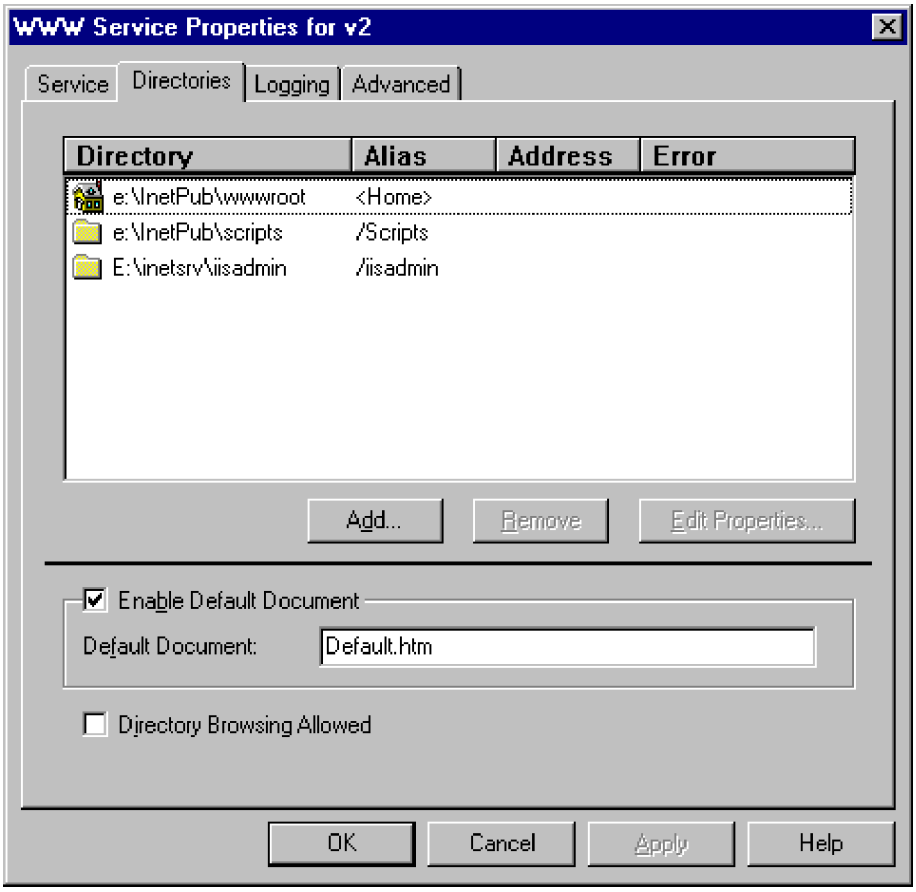


- **Windows NT Challenge/Response** salakirjoittaa automaattisesti käyttäjätunnukset ja salasanat. Internet Explorer 2.0 ja uudemmat tukee tätä ominaisuutta. Jos olet valinnut edellisetkin valinnat, niin tarvittaessa Internet Explorer välittää käyttäjätunnuksen ja salasanan palvelimelle - esimerkiksi jos WWW-palvelimella on käytetty NTFS-suojauksia.

■ **Comment** - antaa kommentin tai kuvauksen palvelulle.

Lisäsuojauksia WWW-vertaispalvelimen käyttöön saa määrittelemällä WWW-vertaispalvelimen käyttämiin kansioihin NTFS-suojauksia. Tällöin **Windows NT haaste/vastaus** (Windows NT Challenge/Response) -menetelmä pääsee oikeuksiinsa.

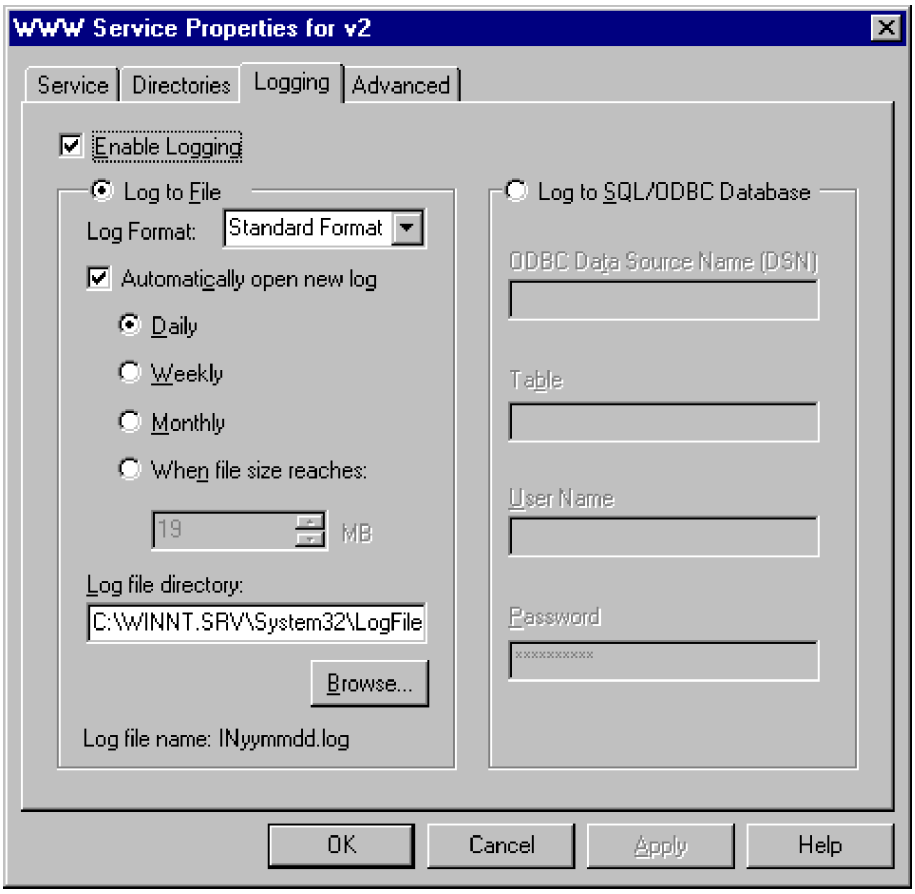
Directories



Directories-välilehdessä voit antaa seuraavat asetukset:

- **Enable Default Document** - valinnalla voit asettaa WWW-palvelimen oletuskotisivun (**Default.htm**)
- **Directory Browsing Allowed** - sallii kansioiden selaamisen
- **Add** -painikkeella voit lisätä hakemistoja
- **Remove** -painikkeella voit poistaa hakemistoja
- **Edit Properties**-painikkeella voit määritellä **näennäis**- eli **virtuaalikansioita**. Tällainen kansio voi sijaita muualla kuin oletuskansiossa.

Logging

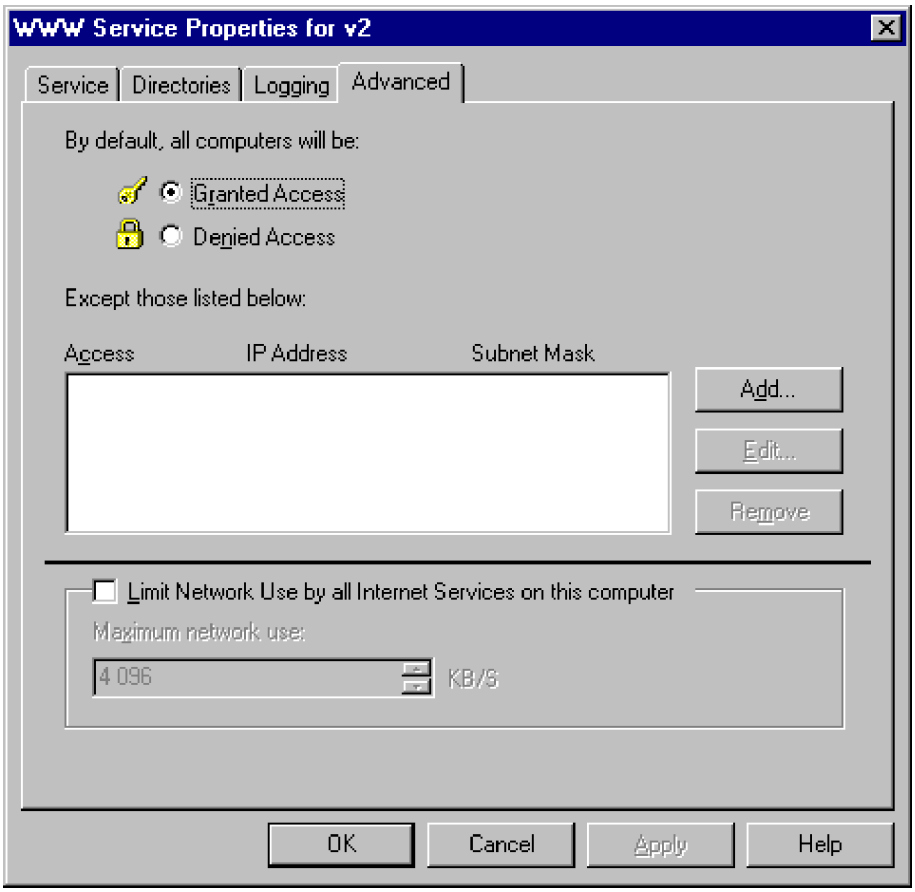


Logging-välilehdessä määritellään lokin asetukset:

- **Enable Logging** - käytetäänkö lokiinkirjoitusta
- **Log to file** - tallennetaan tiedostoon
- **Log to SQL/ODBC Database** - tallennetaan tietokantaan, jolloin voit antaa ODBC-kohteen, taulun ja käyttäjätunnuksen salasanoineen
- **Log format** - lokin muotoilu

- **Automatically open new log** - uuden lokitiedoston luominen:
  - **Daily** - päivittäin
  - **Weekly** - viikoittain
  - **Monthly** - kuukausittain
  - **When the size reaches** - lokin koon saavuttaessa annetun rajan (Mt)
- **Log file directory** - hakemisto, jonne loki tallennetaan - oletuksena tallennetaan hakemistoon **WINNT.-SRV\System32\LogFiles** eli NT:n järjestelmähakemistoon! Kannattanee siirtää toiseen levyasemaan ja/tai hakemistoon tai käyttää lokin tallennusta tietokantapalvelimeen.

Advanced



Advanced-välilehdessä määritellään lisäsuojauksia:

- **Granted Access** on oletus, jolloin myönnetään käyttöoikeudet kaikille tietokoneille, mutta luetteloituihin voit määritellä ne, joilla oikeuksia **ei** ole. Lisääminen tehdään **Add**-painikkeella
- **Denied Access** - luetteloituihin voit määritellä ne, joilla oikeuksia **on.** Jälleen lisääminen tehdään **Add**-painikkeella.
- **Limit Network Use by all Internet Services on this computer** - kaista n rajoittaminen haluttuun määrään kilotavuja sekunnissa, kt/s (**kB/s**).

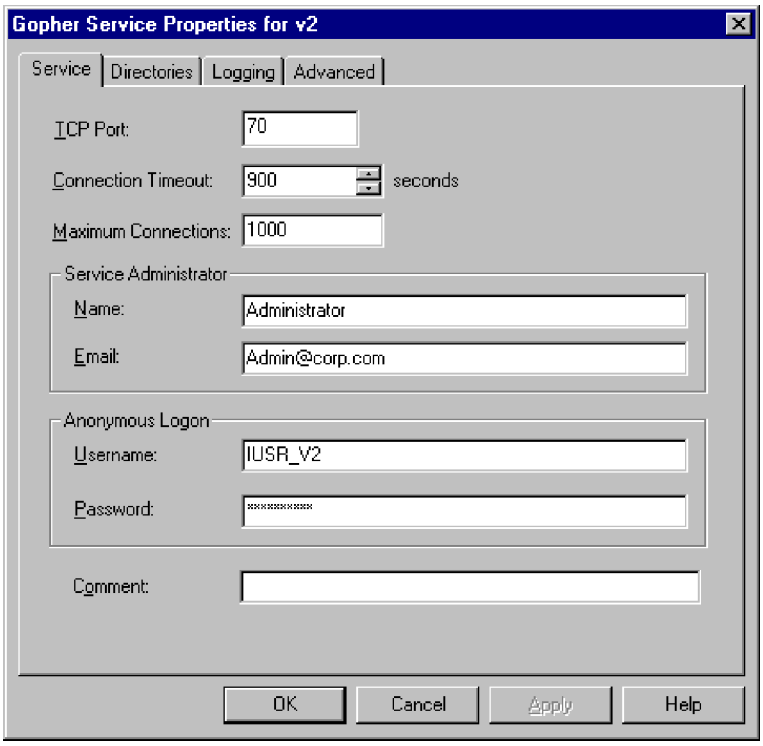
Gopher-palvelimen asetukset

Asetukset ovat lähes identtiset WWW-palvelimen kanssa.

Gopher-palvelimen asetuksissa on neljä välilehteä:

- **Service** - palvelu
- **Directories** - kansio
- **Logging** - loki
- **Advanced** - lisäasetukset.

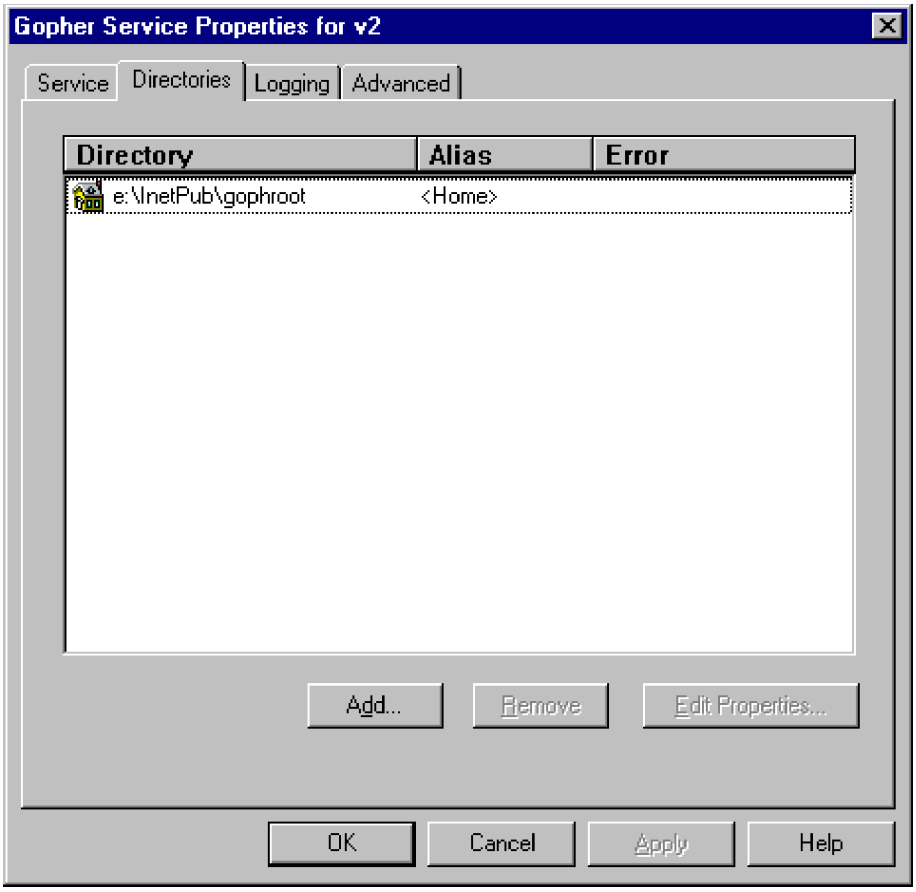
Gopher Service



Service-välilehdessä voit asettaa seuraavat:

- **TCP Port** - palvelimen käyttämän portin numero, oletus **70**
- **Connection Timeout** määrittelee yhteyden aikakatkaisun, jos käyttäjä ei tee mitään annetun ajan kuluessa
- **Maximum Connections** - samanaikaisten käyttäjien maksimimäärä
- **Service Name** - pääkäyttäjän käyttäjätunnus
- **Email** - pääkäyttäjän sähköpostitunnus
- **Anonymous Logon** - oletuksena käytetään paikallista käyttäjätunnusta **IUSR_(palvelimen nimi)**, mikä on annettu **Username**-kohdassa ja **Password** on myös määritelty
- **Comment** - antaa kommentin tai kuvauksen palvelulle.

Gopher Directories



Directories-välilehdessä voit antaa seuraavat asetukset:

- **Add** -painikkeella voit lisätä hakemistoja
- **Remove** -painikkeella voit poistaa hakemistoja
- **Edit Properties**-painikkeella voit muuttaa hakemistojen asetuksia.

Logging

Asetukset ovat samat kuin vastaavassa välilehdessä WWW-palvelimessa.

Advanced

Asetukset ovat samat kuin vastaavassa välilehdessä WWW-palvelimessa.

FTP-palvelimen asetukset

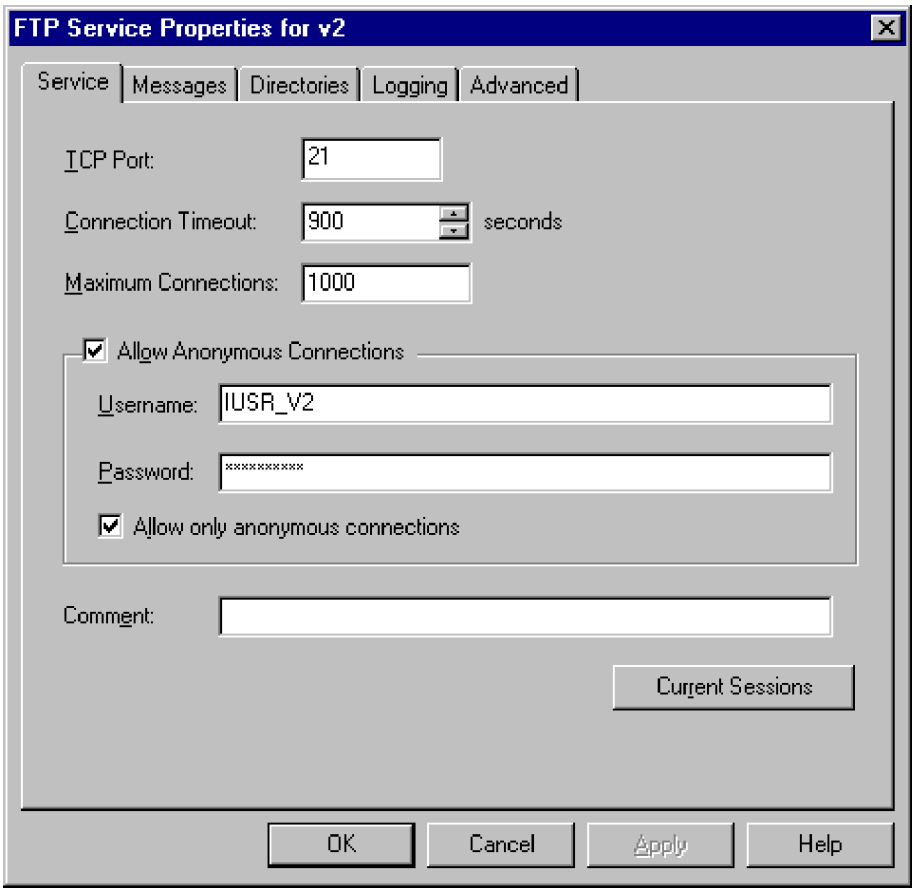
FTP (*File Transfer Protocol*)-palvelin mahdollistaa tiedostojen siirron käyttäen TCP/IP-protokollaa. Kun käyttäjät liittyvät FTP-palvelimeen, käyttäjät voidaan asettaa käyttämään NT-käyttäjätunnuksia ja -salasanoja. Kannattaa myös asentaa FTP-palvelimen tiedostojenjako kiintolevylle, jolle on asennettu NTFS-tiedostojärjestelmä; tällöin saadaan myös kansioiden suojaustaso käyttöön.

FTP-palvelimen asetuksissa (FTP Service Properties) on viisi välilehteä:

- **Service** - palvelu
- **Messages** - sanomat
- **Directories** - hakemistot
- **Logging** - loki
- **Advanced** - lisäasetukset.

Service

Service-välilehdessä voit asettaa seuraavat:



Service-välilehdessä voit asettaa seuraavat:

- **TCP Port** - palvelimen käyttämän portin numero, oletus **21**
- **Connection Timeout** määrittelee yhteyden aikakatkaisun, jos käyttäjä ei tee mitään annetun ajan kuluessa, oletus **900**
- **Maximum Connections** - samanaikaisten käyttäjien maksimimäärä, oletus **1000**
- **Allow Anonymous Connections** - jos käyttäjä ei anna käyttäjätunnustaan, oletuksena käytetään paikallista käyttäjätunnusta **IUSR_(palvelimen nimi)**, mikä on annettu **Username**-kohdassa ja **Password** on myös määritelty

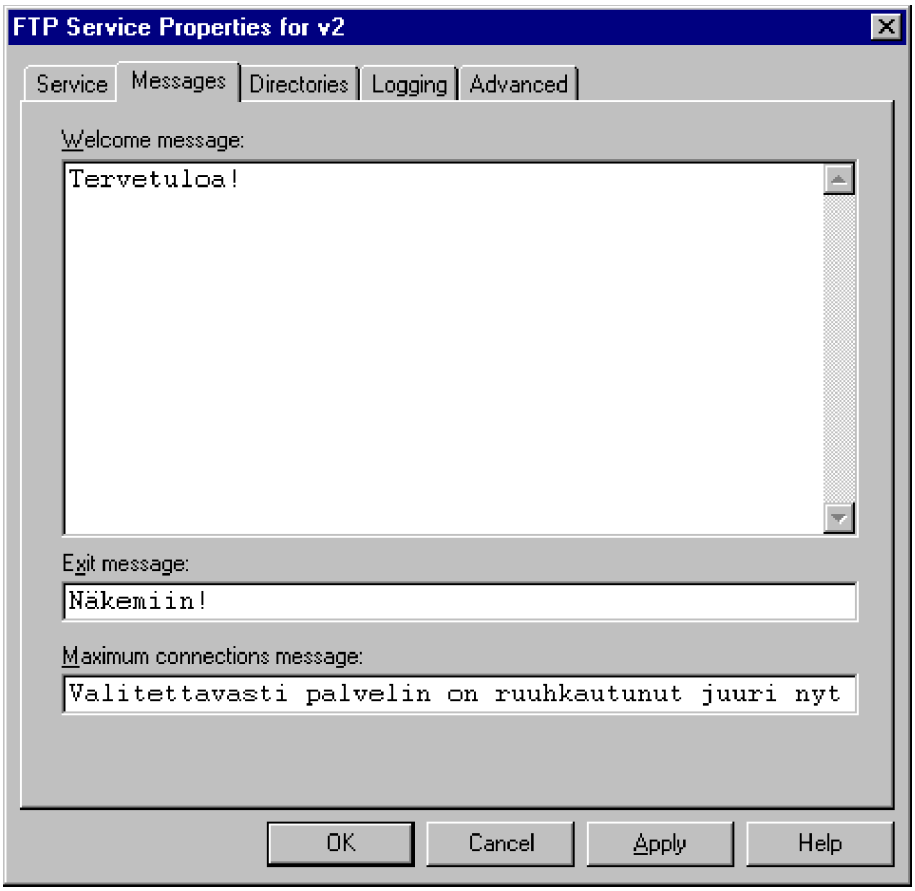
- **Allow only anonymous connections** määrittelee, sallitaanko ainoastaan käyttäjätunnuksettomat nimettömät kirjautumiset. Tällöin vain NT kirjaa kaikki käyttäjät edellisessä kohdassa määritellyllä tunnuksella käyttäjäksi

- **Comment** - antaa kommentin tai kuvauksen palvelulle

- **Current Sessions** - tällä hetkellä kirjautuneet käyttäjät.

Messages

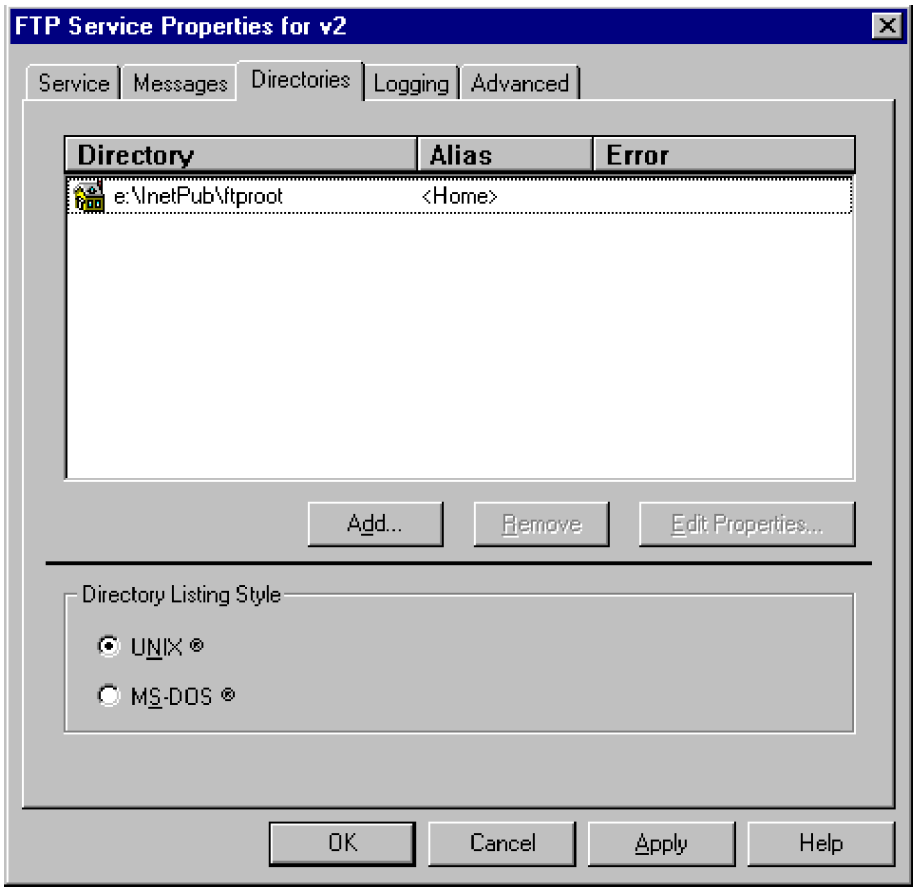
Messages -välilehdessä voit asettaa sanomien seuraavat asetukset:



- **Welcome Message** - näytetään, kun käyttäjä kirjautuu FTP-palvelimeen
- **Exit message** - näytetään, kun käyttäjä kirjautuu pois FTP-palvelimesta
- **Maximum connections message** näytetään, kun sallittu samanaikainen yhteysmäärä on ylitetty.

Directories

Directories-välilehdessä voit asettaa FTP-palvelimen hakemiston.



Valinnat ovat:

- **Add** -painikkeella voit lisätä hakemistoja
- **Remove** -painikkeella voit poistaa hakemistoja
- **Edit Properties**-painikkeella voit muuttaa hakemistojen asetuksia
- **Directory Listing Style** - tiedostolistauksen tyyli: **Unix** tai **MS-DOS**. Se määrittelee listauksen ulkoasun - Unix on useimmissa selaajissa yhteensopivampi kuin MS-DOS-tyylinen listaus.

Logging

Asetukset ovat samat kuin vastaavassa välilehdessä WWW-palvelimessa.

Advanced

Asetukset ovat samat kuin vastaavassa välilehdessä WWW-palvelimessa.

Käyttäjätunnukset

Voit käyttää Windows NT-palvelimen ja -toimialueen suojausominaisuuksia yhdessä Internet Information Serverin hakemistojen käyttöoikeusvalvonnan kanssa. Näin voit valvoa, kuinka laajasti WWW-käyttäjät voivat päästä palvelimellesi. Seuraavaksi käsitellään näiden ominaisuuksien käyttöönottoa.

Muista seuraavat periaatteet:

- Kannattaa perehtyä Windows NT:n suojauksiin, käyttöoikeuksiin ja käyttäjäryhmiin. Palvelimesi tietoturva riippuu paljolti siitä, että tiedät mitä käyttäjät voivat tehdä kirjauduttuaan käyttäjäoikeuksillaan

- Kun luot käyttäjiä User Manager for Domainsilla, anna käyttäjätunnukselle salasana. Voit pakottaa käyttäjät muuttamaan salasanaansa, kun he kirjautuvat sisään ensimmäisen kerran. Voit myös pakottaa heidät muuttamaan salasanaansa haluamasi ajan kuluttua

- Pidä huolta palvelimiesi pääkäyttäjien oikeuksista. Älä jätä palvelinta ilman silmälläpitoa äläkä anna salasanoja *yleiseen jakeluun*

- Jos peruskäyttäjät tai tukihenkilöt vastaavat joidenkin toimintojen ylläpidosta palvelimella, älä anna näiden käyttäjätunnuksille yhtään enempää oikeuksia kuin on tarpeen. Tarkista hakemistojen käyttöoikeudet

- Ota käyttöön asetukset, jotka rajoittavat epäonnistuneiden kirjautumisyritysten määrää ennen kuin käyttäjätunnus suljetaan. Näin estetään tunkeilijoita yrittämästä useita salasanoja heidän yrittäessään päästä järjestelmään.

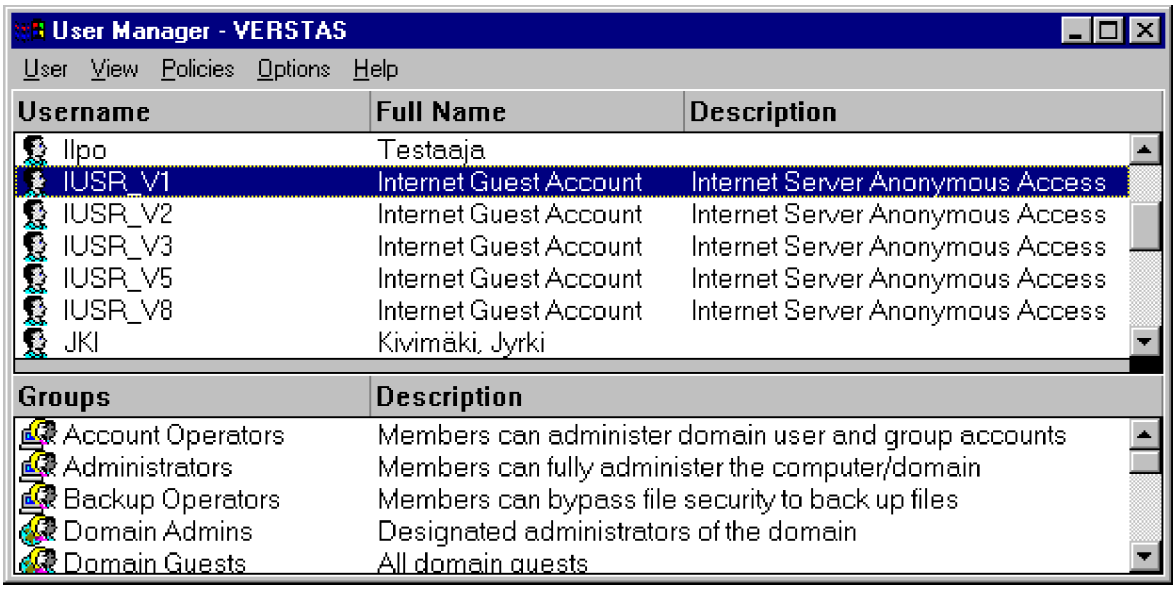
IUSR_palvelin

Toimialueella käyttäjätunnukset tallennetaan ensisijaiseen toimialueen ohjauskoneen (*Primary Domain Controller*, PDC) käyttäjätietokantaan, josta ne monistetaan toimialueen ohjauskoneen varakoneiksi (*Backup Domain Controller*, BDC). Kun käyttäjät kirjautuvat käyttäjätunnuksella, he kirjautuvat toimialueelle eivätkä yksittäiseen palvelimeen.

Kun Internet Information Server asennetaan, toimialueen käyttäjätietokantaan luodaan **IUSR_palvelimen nimi**-käyttäjätunnus. Käyttäjätunnusten ylläpito tapahtuu **User Manager for Domainsilla**. Jos käyttäjätunnus luodaan **Stand-alone Server**-tyyppisessä palvelimessa (siis ei toimialueen ohjauskoneessa), käyttäjätunnus luodaan paikalliseen käyttäjätunnustietokantaan. Silloin käyttäjätunnuksen ylläpitoon käytetään kyseisen palvelimen User Manager for Domainsia. Jos käyttäjätunnus luodaan NT-työasemaan, käytetään NT-työaseman User Manager-ohjelmaa.

User Managerissa ei ole ominaisuuksia toimialueen käyttäjätunnuksien ylläpitoon.

Jos Internet Information Server asennetaan toimialueella usealle eri palvelimelle, päädytään sinänsä mielenkiintoiseen tilanteeseen - toimialueen käyttäjätunnustietokantaan luodaan kullekin palvelimelle käyttäjätunnus käyttämällä **IUSR_palvelimen nimi**-muotoa.



Tämä ei sinällään ole ongelma, mutta helpottaaksesi ylläpitoa haluat ehkä käyttää vain yhtä käyttäjätunnusta kaikissa Internet Information Servereissä.

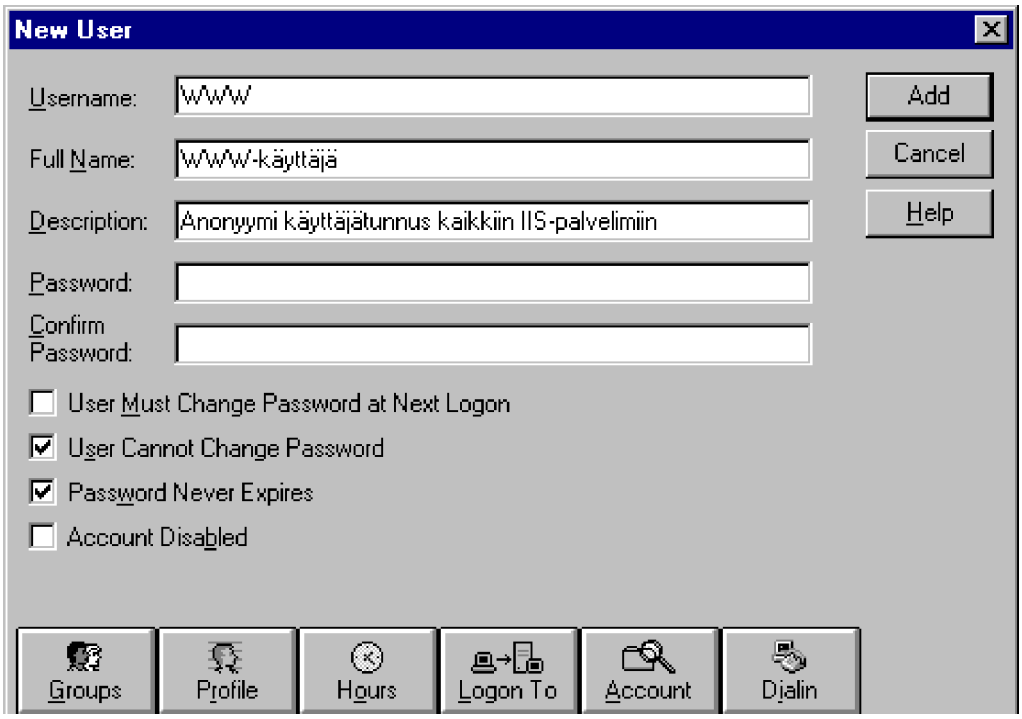
Tällöin toimitaan seuraavasti:

1) Käynnistä **User Manager for Domains**

2) Valitse **User** | **New User**

3) Täytä käyttäjätunnus-, salasana- ja kuvauskentät

4) **Poista** valinta **User Must Change Password at Next Logon** ja valitse **User Cannot Change Password**- ja **Password Never Expires** -valinnat

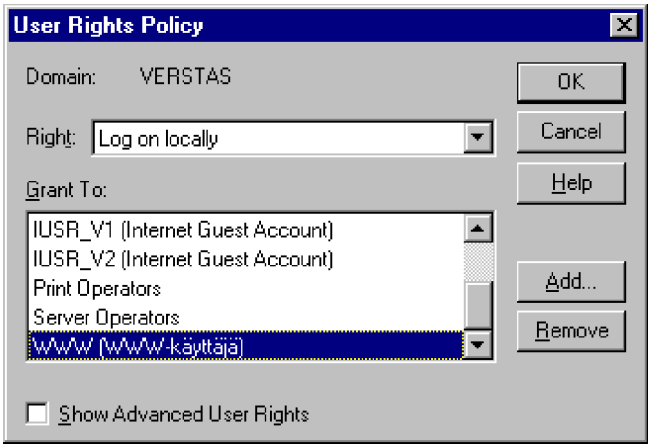


5) Valitse **Groups**-painike ja varmista, että käyttäjätunnus kuuluu ryhmään (esim. Guests- tai mikä tahansa muu ryhmä), jolla on luku- tai suoritusoikeudet WWW-palvelimen hakemistoihin

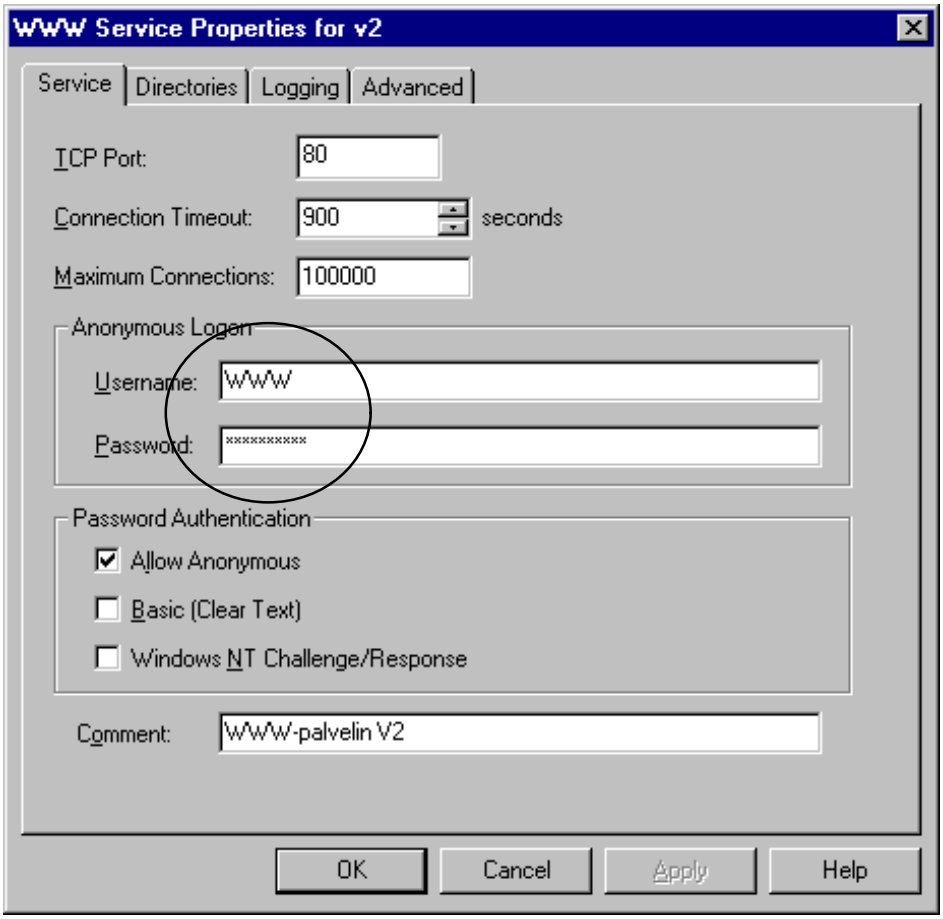
6) Valitse **OK**, jolloin käyttäjätunnus luodaan

7) Valitse **Policies** | **User Rights**, jolloin avautuu **User Rights Policies** -valintaikkuna.

8) Valitse **Right**-kentästä **Log On Locally** ja valitse sitten **Add**-painike ja lisää uusi käyttäjätunnus



9) Avaa **Internet Service Manager** ja kaksoisnapauta WWW-palvelinta, jolloin ominaisuussivu aukeaa. Kirjoita **Service**-sivulla **Anonymous Logon** -kenttään uusi käyttäjätunnus ja salasana. Tarkista myös, että **Allow Anonymous** on valittu

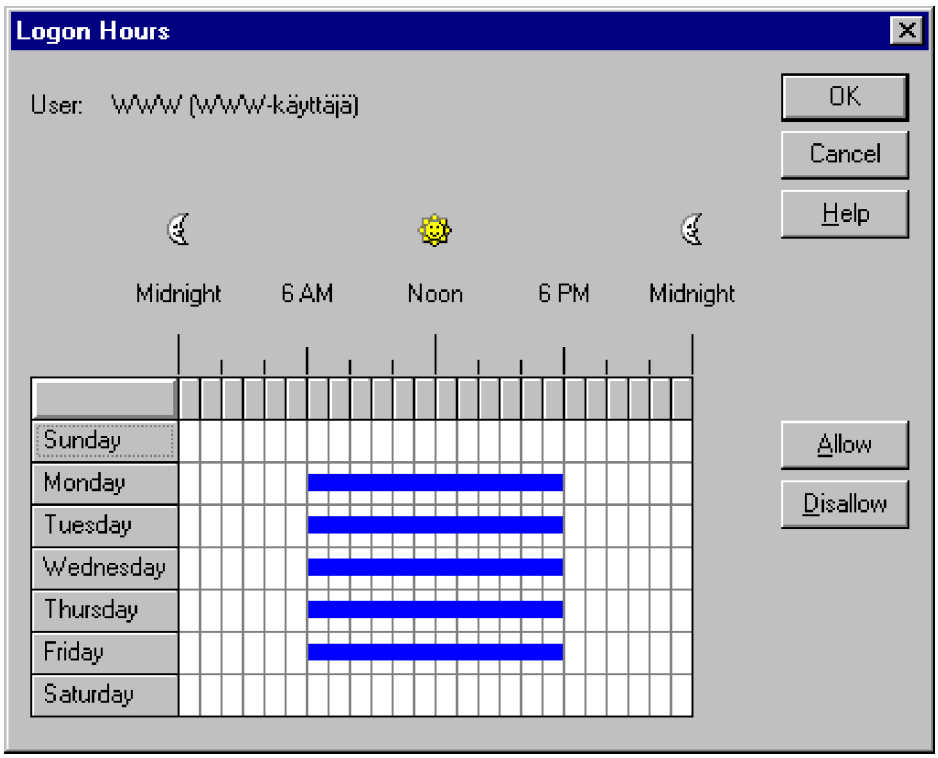


10) Toista edellisen kohdan toimet kussakin toimialueella toimivassa Internet Information Serverissä.

Jos myöhemmin asennat samalla toimialueella lisää Internet Information Servereitä, voit määritellä saman anonyymin käyttäjätunnuksen kuin edellä.

Tarkista, että **IUSR_palvelimennimi**-käyttäjätunnuksella ja kaikilla muilla (myös itse luomillasi) palvelinta käyttävillä käyttäjätunnuksilla on vain ne oikeudet, jotka ne tarvitsevat, mutta ei enempää!

Voit esimerkiksi rajoittaa tämän käyttäjätunnuksen **kirjautumisaikoja** (*Hours*), mutta olepa tarkkana ettet sotkeudu tässä asiassa samalla eri kirjausmenettelyjen viidakkoon!



Laajimmillaan **IUSR_palvelin**-käyttäjätunnuksella, **Everyone**- ja **Guests**-ryhmillä on kaikilla oikeus kirjautua järjestelmään paikallisesti.

Voit tarkistaa tämän edellisillä toimenpiteillä **7)** - **8)**.

Lisäksi **Everyone**-tai **Domain Users** -ryhmällä pitäisi olla oikeus **Access This Computer from Network**, niin että verkkokäyttäjät voivat kirjautua palvelimelle sisäisen verkon NT-työasemalta tai etäpalvelimelta. Huomaa, että anonyymeillä käyttäjillä on edelleenkin pääsy WWW-sivuille, vaikka tämä oikeus ei olisikaan käytössä.

Jos haluat tehostaa tietoturvallisuutta, poista **Everyone**- ja **Guests**-ryhmiltä **Log On Locally** -oikeus, ja anna sen sijaan **IUSR_palvelinnimi**-käyttäjätunnukselle **Log On Locally** -oikeus.

Lisäksi IIS:n hakemistojen oikeuksien tulisi olla kunnossa. Windows NT 4.0:ssa oikeudet voi tarkistaa hakemiston oikeudet napauttamalla hakemistoa hiiren oikealla painikkeella, valitsemalla esiin tulevasta pikavalikosta **Properties**, sitten **Security**-välilehti ja lopuksi **Permissions**-paini-

ke. Näet luettelon käyttäjistä ja ryhmistä, joilla on oikeus tähän hakemistoon. Voit lisätä ryhmiä valitsemalla **Add**-painikkeen tai poistaa niitä valitsemalla **Remove**-painikkeen. Jos haluat muuttaa olemassa olevan käyttäjätunnuksen ominaisuuksia, valitse se hiirellä ja valitse sitten uudet oikeudet **Type of Access** -ruudusta.

Käyttäjätunnusten asetuksia on käsitelty luvussa **5**.

Suojauksia on käsitelty luvussa **11**.

Anonyymi käyttäjätunnus

Kaikki WWW-sivuillesi saapuvat käyttäjät kirjautuvat **oletuksena** käyttäen **anonyymiä käyttäjätunnusta** (IUSR_palvelimen nimi). Tunnus luodaan automaattisesti Internet Information Serverin asennuksen yhteydessä. Teknisesti ottaen anonyymi yhteys muodostetaan, kun WWW-pyynnön (HTTP) otsikkotiedoissa **ei ole käyttäjätunnusta ja salasanaa** - tämä on useimpien selainten oletusasetus uusille WWW-yhteyksille.

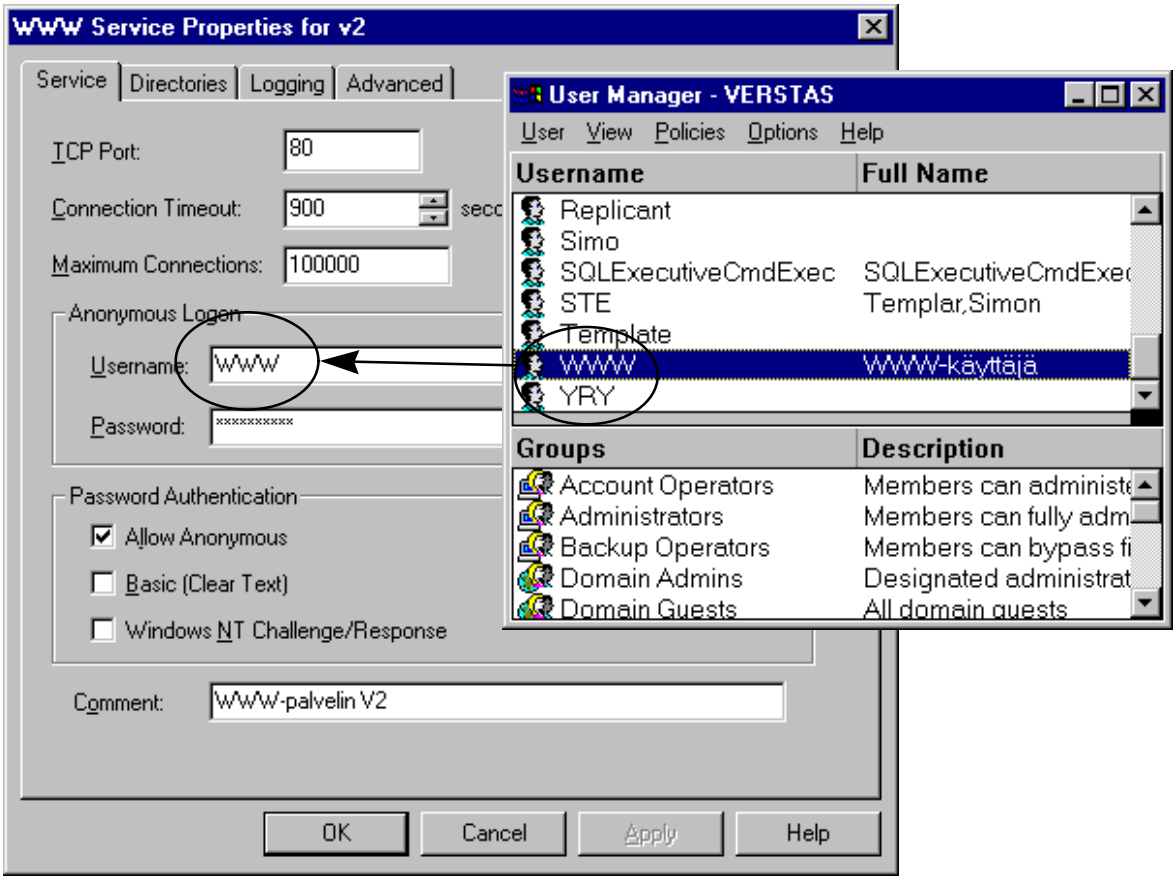
Anonyymiä käyttäjätunnusta käytettäessä käyttäjien ei tarvitse antaa käyttäjätunnusta tai salasanaa, jolloin käyttäjät pääsevät palvelimelle helposti. Haittapuoli kuitenkin on se, että et voi tietää keitä palvelimellasi käy, koska kaikilla kävijöillä on sama käyttäjätunnus.

Kuitenkin myös anonyymitunnusta käytettäessä kaikissa Internet Information Serveriä käyttävän järjestelmän toiminnoissa määritetään lupia käyttäjätunnuksen perusteella. Käyttäjätunnuksen yhdistäminen jokaiseen toimintoon on Windows NT:n turvallisuuden yksi perusperiaate.

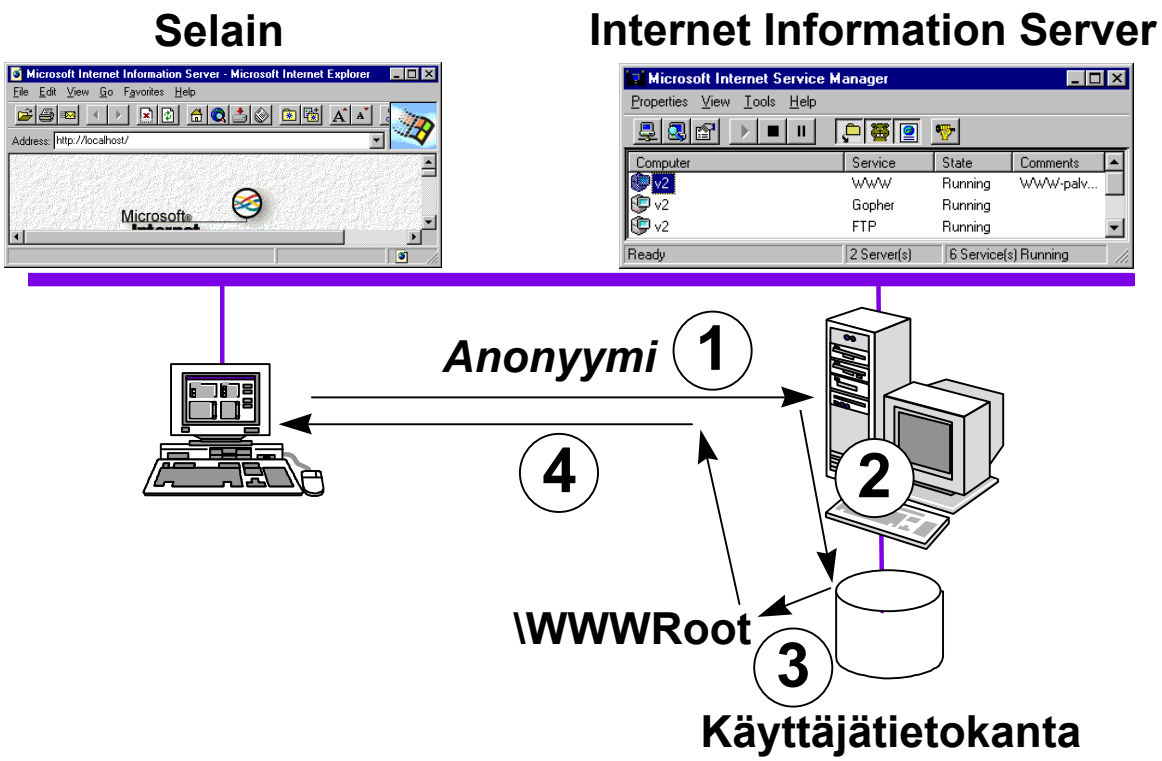
Internet Information Serverin asennuksen aikana luodulle **IUSR_palvelinnimi**-tunnukselle luodaan **satunnaissalasana**. Tunnus lisätään paikalliseen tai toimialueen käyttäjätietokantaan, ja käyttäjätunnusta voidaan muuttaa User Manager for Domainsin avulla.

Internet Explorer ja useimmat muut selaimet eivät anna käyttäjätunnusta ja salasanaa ottaessaan yhteyttä WWW-palvelimeen, joten Internet Information Server käyttää **IUSR_palvelinnimi**-tunnusta,

Service-sivulla **IUSR_palvelinnimi**-tunnukselle tai muulle käyttäjätunnukselle määritettyjen käyttäjätietojen täytyy olla yhtäläiset User Manager for Domainsissa annettujen saman tunnuksen asetusten kanssa. Käyttö estetään, jos käyttäjätunnus ja salasana eivät täsmää.



Jos halutaan sallia **vain anonyymikäyttö** mikä on useimmiten suositeltavaa tyhjennetään valintaruudut **Basic (Clear Text)** ja **Windows NT Challenge/Response**. Jos **vain** anonyymikäyttö sallitaan, kukaan ei voi käyttää Windows NT -käyttäjätunnusta väärin, koska tällöin estetään kirjautuminen esimerkiksi Administrator-tunnuksella, jolla taas on riittävästi oikeuksia toimialueella.



Kirjautuminen anonyymilla käyttäjätunnuksella toimii seuraavasti:

1) Käyttäjä pyytää esim. WWW-sivua

2) IIS välittää pyynnön käyttämällä **IUSR_palvelinnimi**-tunnusta, tarkistus tehdään käyttäjätietokannasta

3) **IUSR_palvelinnimi** hakee sivun resurssista (jos oikeudet riittävät), esimerkissä **WWWRoot**-hakemistosta

4) Joko **WWW-sivu** tai **käyttö kielletty** (Access Denied) palautetaan käyttäjälle.

Huomaa:

- Kaikki WWW-asiakkailta tulevat pyynnöt käyttävät tätä käyttäjätunnusta, jos sallit **vain** anonyymit kirjautumiset
- IIS vaihtaa jokaisen kirjautumisen yhteydessä anonyymin käyttäjätunnuksen salasanan - niinpä sen arvaaminen on tilastollisesti katsoen lähes mahdotonta

- Oletuksena käyttäjä ei voi poistaa tai muuttaa tiedostoja NTFS-tiedostojärjestelmässä, koska hänellä on vain **lukuoikeus** (tai tiedostojen suoritusoikeus skripti- ja ohjelmahakemistoissa) WWW-palvelimen hakemistoihin

- Koska käyttäjällä on vain rajalliset oikeudet, käyttäjät eivät voi siirtää tiedostoja palvelimelle ja suorittaa ohjelmia kuin määritellyissä hakemistoissa

- **Toimialueella** (*Domain*) tämä käyttäjätunnus lisätään toimialueen PDC:n käyttäjätietokantaan

- Muilla WWW-palvelimillasi on samanlaiset anonyymit käyttäjätunnukset, mutta tarvittaessa voit luoda koko toimialueelle **yhden yhteisen anonyymin käyttäjätunnuksen**

- Jos estät **Everyone**-ryhmän pääsyn WWW-palvelinhakemistoon, anonyymit käyttäjät eivät myöskään pääse sinne, ellet erityisesti lisää anonyymiä internet-kävijän käyttäjätunnusta (**IUSR_palvelimen nimi**) hakemistoon ja myönnä sille luku- tai suoritusoikeutta riippuen hakemiston käyttötarkoituksesta.

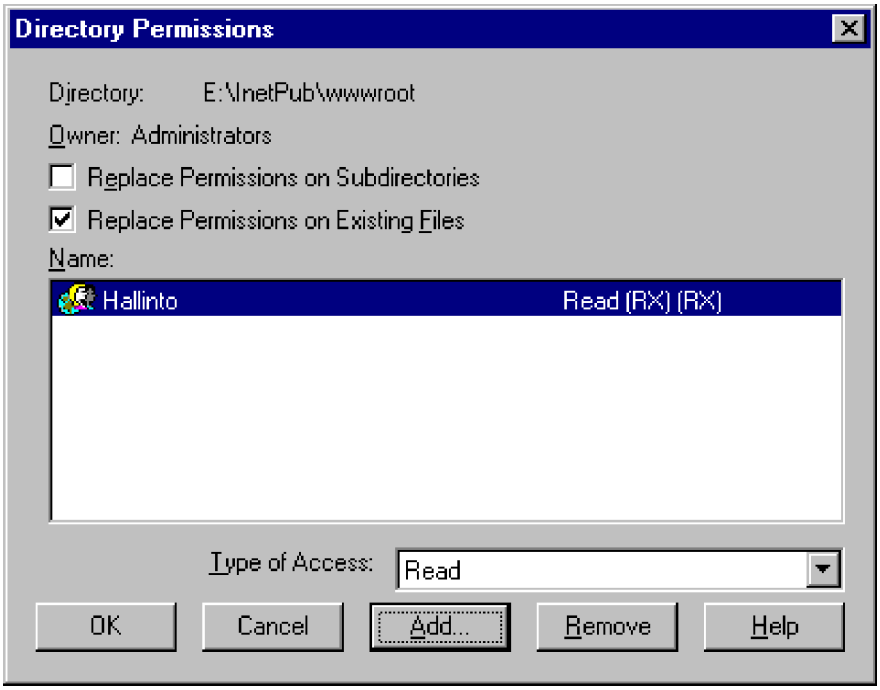
Käyttäjätunnuksen vaatiminen kirjauduttaessa

Windows NT-palvelimissa käyttäjätunnukset luodaan User Manager for Domainsilla ja käyttäjätunnuksille myönnetään erityisiä oikeuksia resurssien käyttöön.

Voit ottaa käyttöön käyttäjien kirjautumismenettelyn seuraavalla menettelyllä, kun käyttäjät kirjautuvat WWW-palvelimeesi:

1) Rajoita anonyymien käyttäjien hakemistojen käyttöoikeutta poistamalla **Everyone**-, **Guest**- ja **IUSR_koneennimi-tunnukset** hakemiston käyttöoikeuslistasta

2) Lisää käyttäjätunnus tai käyttäjäryhmä, jolle haluat antaa hakemiston käyttöoikeuden ja jolle haluat antaa haluamasi käyttöoikeudet valitsemalla oikeudet **Type of Access** -listasta

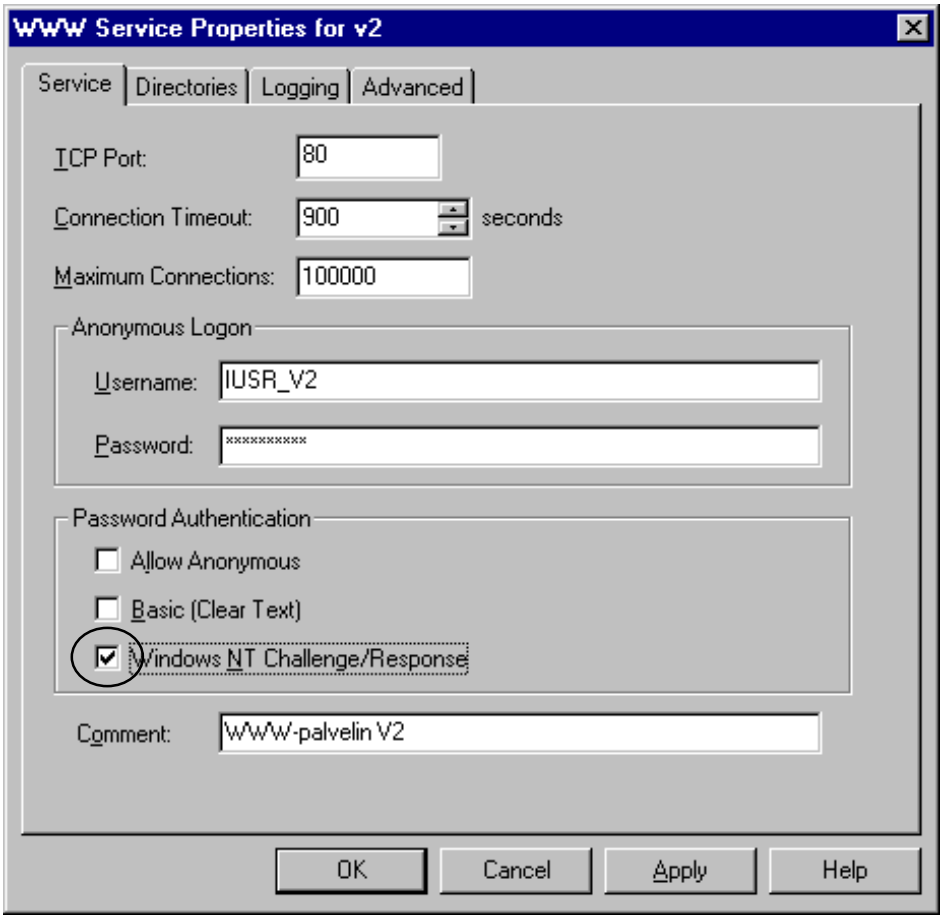


3) Ota **Internet Service Managerissa** käyttöön **Basic**- tai **Challenge/Response**-tunnistus. Tämä tehdään seuraavaksi. Kaksoisnapauta WWW-palvelinta ja avaa Service-valintaikkuna. Password Authentication -ryhmässä on kolme tasoa:

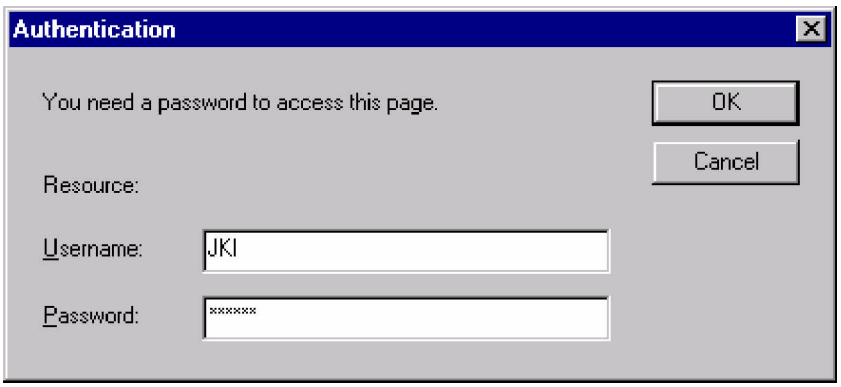
- **Allow Anonymous** - internet-käyttäjien vieras/anonyymi käyttäjä -vaihtoehto. Kun tämä vaihtoehto on valittu (oletus), käyttäjät voivat käyttää hakemistoja, joihin Everyone-, Guest-, Interactive- ja IUSR_koneennimi-käyttäjätunnuksilla on käyttöoikeudet. Jos **Allow Anonymous** on valittu ja **Basic**- ja **Windows NT Challenge/Response**-valintaruudut ovat molemmat tyhjiä, kaikki asiakkaiden pyynnöt käsitellään anonyymeinä pyyntöinä, vaikka käyttäjä antaisikin käyttäjätunnuksen ja salasanan. Jos poistat valinnan tästä ruudusta, sinun on valittava jompikumpi tai molemmat kahdesta muusta valintaruudusta. Silloin kaikkien käyttäjien on kirjautuessaan annettava käyttäjätunnus ja salasana, ja sinun on luotava heille sopivat käyttäjätunnukset WWW-palvelimelle ennen kuin kukaan käyttäjistä voi kirjautua

- **Basic (Clear Text)** - valitse Basic-vaihtoehto, niin käyttäjät voivat yrittää kirjautua suojattuihin hakemistoihin. Tällöin käyttäjä on kirjautunut hakemiston käyttäjäksi tavallaan rekisteröitynä käyttäjänä. Yleensä anonyymien käyttäjien annetaan kirjautua ainoastaan lukuoikeuksilla hakemistoihin, joissa on vain rekisteröityjen käyttäjien luettaviksi tarkoitettuja sivuja. Suurin ero tämän ja **Windows NT Challenge/Response**-valinnan välillä on se, että käyttäjätunnukset ja salasanat lähetetään selväkielisinä **ilman vahvaa salausta**. Koodauksessa käytetään **uuencode**-nimistä koodausta, jonka määrätietoinen krakkeri pystyy murtamaan suhteellisen helposti. **Basic**-tunnistus on kuitenkin yleensä riittävä silloin, kun julkaistu tieto ei ole luottamuksellista, ja haluat vain sen verran käyttäjävalvontaa, että käyttäjien on kirjauduttava käyttäjätunnuksella. Tällä tavoin voit pitää kirjaa siitä, kuka järjestelmääsi käyttää. Anonyymeillä käyttäjätunnuksilla tämä ei ole mahdollista.

- **Windows NT Challenge/Response** - asetuksella NT-toimialueelle jo kirjautuneille käyttäjille annetaan automaattisesti käyttöoikeudet niihin hakemistoihin, joihin heidän käyttäjätunnuksillaan on käyttöoikeus. **Windows NT Challenge/Response** -protokolla muuntaa verkossa lähetettävät salasanat salakielisiksi.



Jos kirjautuminen ei onnistu **Windows NT Challenge/Response** -käyttäjätunnistusmallia käyttäessäsi,niin tarkista tarvittaessa, että **INTERACTIVE**- ja **NETWORK**-ryhmillä on käyttöoikeudet niissä hakemistoissa, jotka haluat tällä mallilla suojata.



Microsoft kehittelee ylläpitotuotteita, joiden avulla pääkäyttäjät voivat käyttää ylläpitotyökaluja kirjautumalla WWW-palvelimille WWW-selaimilla Windows NT Challenge/Response -menetelmää käyttäen.

Kirjautumismekanismi

Kun käyttäjät kirjautuvat Internet Information Server -palvelimien suojattuihin hakemistoihin käyttämällä **Basic (Clear Text)**- tai **Windows NT Challenge/Response**-käyttäjätunnistusmallia, kirjautumismekanismi toimii seuraavasti:

1) Aluksi käyttäjä yrittää päästä suojattuun hakemistoon anonyymikäyttäjä -pyynnöllä. Pyyntö epäonnistuu, koska anonyymillä käyttäjällä ei ole tarvittavia oikeuksia hakemistoon pääsemiseksi

2) Palvelin vastaa käyttäjälle osoittamalla, minkätyyppistä käyttäjätunnistusmallia se tukee

3) Käytössä olevasta turvajärjestelmästä riippuen selain tekee jomman kumman seuraavista:

- Jos käytössä on **Basic (Clear Text)** -käyttäjätunnistus ja selain tukee sitä, näytetään valintaikkuna, jossa pyydetään käyttäjätunnus ja salasana. Alkuperäinen pyyntö hakemistoon pääsystä toistetaan niin, että käyttäjätiedot ovat mukana pyynnössä

- Jos käytössä on **Windows NT Challenge/Response**-käyttäjätunnistus ja selain tukee sitä, selain automaatisesti uudelleenlähettää alkuperäisen pyynnön takaisin palvelimelle siten, että käyttäjätiedot ovat mukana pyynnössä.

Kirjautumisasetukset

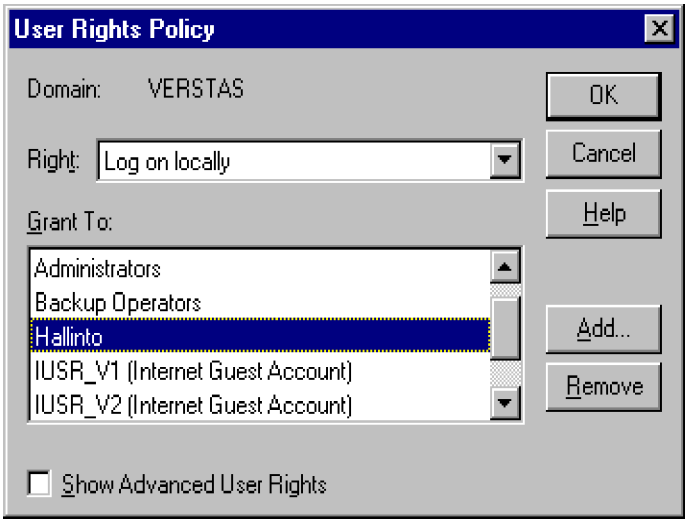
Jos haluat WWW-käyttäjien antavan käyttäjätunnuksen ja salasanan halutessaan päästä johonkin WWW-palvelimesi tiettyyn hakemistoon, tarkista seuraavat asetukset:

- Käyttäjätunnuksen on oltava **Internet Information Server** -palvelimen ymmärtämä kelvollinen käyttäjätunnus:

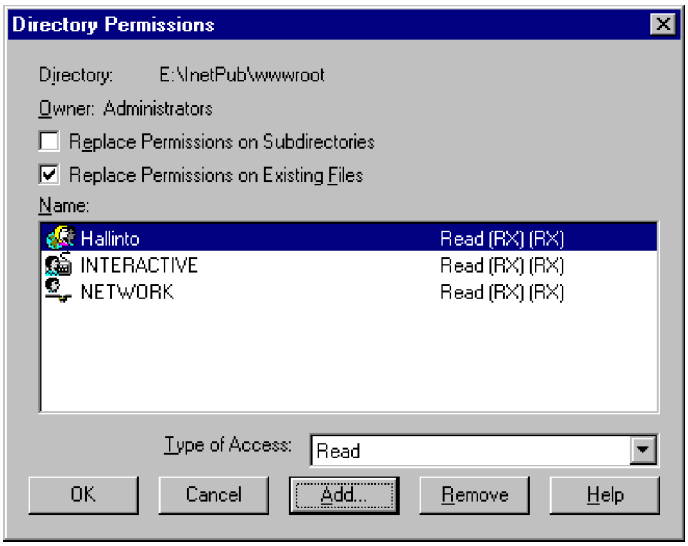
  - Luo käyttäjätunnus **User Manager for Domains**illa (varsinkin jos kyseessä on **Stand-alone Server**-tyyppinen palvelin)

- Käyttäjätunnuksen on oltava Windows NT -toimialueen käyttäjätunnus ja **Internet Information Serverin** on pystyttävä käyttämään toimialueen käyttäjätietokantaa.

■ Käyttäjällä on oltava oikeus kirjautua paikallisesti (**Log On Locally**), mikä voidaan määritellä User Manager for Domainsin **Policies** | **User Rights** -valinnalla. Voit myös varmistaa, että käyttäjä on sellaisen ryhmän jäsen, jolla on tämä oikeus



■ Anna luomallesi käyttäjälle luku-, suoritus- tai muut oikeudet hakemistoon, jossa olet rajoittanut anonyymien käyttäjien käyttöoikeuksia. Varmista, että **INTERACTIVE**- ja **NETWORK**-ryhmillä on käyttöoikeudet myös näihin hakemistoihin



- Ota käyttöön **Basic (Clear Text)** -salasanavarmistus tai **Windows NT Challenge/Response** -käyttäjätunnistus Internet Service Managerin Service-välilehdessä aiemmin esitetyllä tavalla.

Paikallinen kirjautumisoikeus

Log On Locally -käyttöoikeus täytyy myöntää User Managerissa tai User Manager for Domainsissa kaikille käyttäjätunnuksille, jotta ne voivat käyttää Internet Information Serveriä. Internet Information Server käyttää seuraavanlaisia käyttäjätunnuksia:

- Anonyymikäyttäjätunnus (IUSR_koneennimi -tunnus)
- Virtuaalihakemistoja luotaessa määritetyt tunnukset
- Tietokantojen käyttöä varten .idc -tiedostoissa määritetyt tunnukset
- Asiakaskoneilla määritetyt käyttäjätunnukset.

Käytettäessä **Basic (Clear Text)** -salasanavarmistusta IIS kirjaa käyttäjät paikallisina käytäjinä (siksi Log On Locally-oikeus). Internet Information Server 2.0:ssa tai uudemmassa asetusta voidaan muuttaa, jos **Windows NT Challenge/Response** -käyttäjätunnistus ei ole käytössä.

Kirjautumisasetukset ovat rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\W3SVC\Parameters**
Nimi	**LogonMethod**
Tyyppi	**REG_DWORD**
Arvo	**0** - **Log on Locally** (paikallinen käyttäjä), kirjautumissalasana tarvitaan **1** - **Log on as Batch** (kuten edellinen, mutta käyttäjä kirjautuu pois prosessin tai säikeen päättyessä) **2** - **Log on as Network** (etäkäyttäjä, verkko, käyttäjä - voidaan käyttää salakirjoitettua varmennusta)

Internet ja Intranet

Palataanpa vielä käyttäjätunnustukseen. Miten Windows NT -käyttäjätunnuksia konfiguroidaan ja käytetään, määräytyy myös seuraavista seikoista:

- Selainten (*Browser*) tukemat käyttäjäntunnistusmenetelmät
- Käytetäänkö käyttäjäntunnistusta Intranetissa vai Internetissä.

Windows NT:n käyttäjätunnuksien avulla voidaan valvoa koko palvelimen käyttöoikeuksia tai pääsyä tiettyihin tiedostoihin tai hakemistoihin. Kun **Service**-sivun **Allow Anonymous**-valintaruutu on tyhjennetty, kirjautumisikkuna tulee esille aina, kun selain tekee pyynnön palvelimelle.

Jos **Allow Anonymous** on valittu ja **Basic (Clear Text)** tai **Windows NT Challenge/Response** on myös valittu, käyttäjältä pyydetään käyttäjätunnusta ja salasanaa **vain**, jos käyttäjä yrittää päästä NTFS -levyllä olevaan resurssiin **ja** jos resurssin ominaisuuksissa ei sallita pääsyä **IUSR_palvelimennimi**-tunnuksella.

Internet Information Serveriä käyttäville tunnuksille täytyy myöntää **Log On Locally** -käyttöoikeus riippumatta siitä, onko tunnus määritetty Internet Information Serverissä vai antaako käyttäjä käyttäjätunnuksen ja salasanan. Tarkista, että oikeus on annettu niille käyttäjätunnuksille,

joilla käytetään Internet Information Serveriä.

Oikeuksien tarkistaminen intranetissa

Oikeuksien tarkistaminen on helpointa Intranetissä, jos käytössä on jo Windows NT -käyttäjätunnusjärjestelmä. Koska Internet Information Server käyttää Windows NT:n käyttäjätunnuksia, voidaan käyttää toimialueen olemassa olevia käyttäjätunnuksia ja hakemistorakennetta, ja käyttäjätunnuksia voidaan hallita User Manager for Domainsin avulla.

Jos kaikilla selaimet ovat Internet Explorerin 2.0 tai uudempia, voidaan käyttää Windows NT:n turvatun tunnistuksen **Windows NT Challenge/Response**-menetelmää.

Jos valitaan **Windows NT Challenge/Response**, kaikki pyynnöt Internet Explorer 2.0 tai uudemmasta käyttävät tätä menetelmää. Muut selaimet voivat ottaa yhteyden ainoastaan käyttämällä perustason käyttäjätunnistusta, jolloin **Basic (Clear Text)**-valintaruutu täytyy valita.

Windows NT Challenge/Response-menetelmää ei voi käyttää, jos selaimet ovat Internet Explorer versio 1.5 tai vanhempia versiota tai jos käytetty selain ei tue **Windows NT Challenge/Response**-menetelmää.

Jos intranetin turvallisuus huolestuttaa, käyttäjätunnistusta voidaan käyttää yhdessä **Secure Sockets Layerin** (SSL) kanssa. SSL salakirjoittaa tunnistusprosessin myös kaiken selaimen ja palvelimen välisen liikenteen, joten se voi vaikuttaa palvelimen toimintaan.

Oikeuksien tarkistaminen Internetissä

Intranetin käyttäjätunnistuksen periaatteet pätevät myös käyttäjätunnistukseen internetin kautta. Koska ei kuitenkaan voida olettaa, että kaikki Internetin selaimet ovat (ainakaan vielä) Internet Explorer 2.0 tai uudempia, täytyy käyttää **Basic (Clear Text)**-tunnistusta käyttää yhdessä SSL:n kanssa.

Jos tulet luomaan tuhansia käyttäjätunnuksia Internet-käyttäjille, suuren käyttäjämäärän aiheuttamat laitteistovaatimukset täytyy ottaa huomioon.

Hakemistot

Voit suunnitella erilaisia hakemistorakenteita Internet Information Serverille WWW-aineistosi, tietoturvallisuusvaatimustesi tai molempien mukaan.

Hakemistorakenne

Ensimmäisessä esimerkissä **\WWWRoot**-hakemistossa on **WWW**-palvelimen kotisivu. Muut sivut on tallennettu alihakemistoon **\DATA**. **CGI**- ja **ISAPI**-ohjelmat on tallennettu **\PROGRAMS**-hakemistoon:

Päähakemisto	Alihakemistot
\WWWRoot	\DATA
	\PROGRAMS

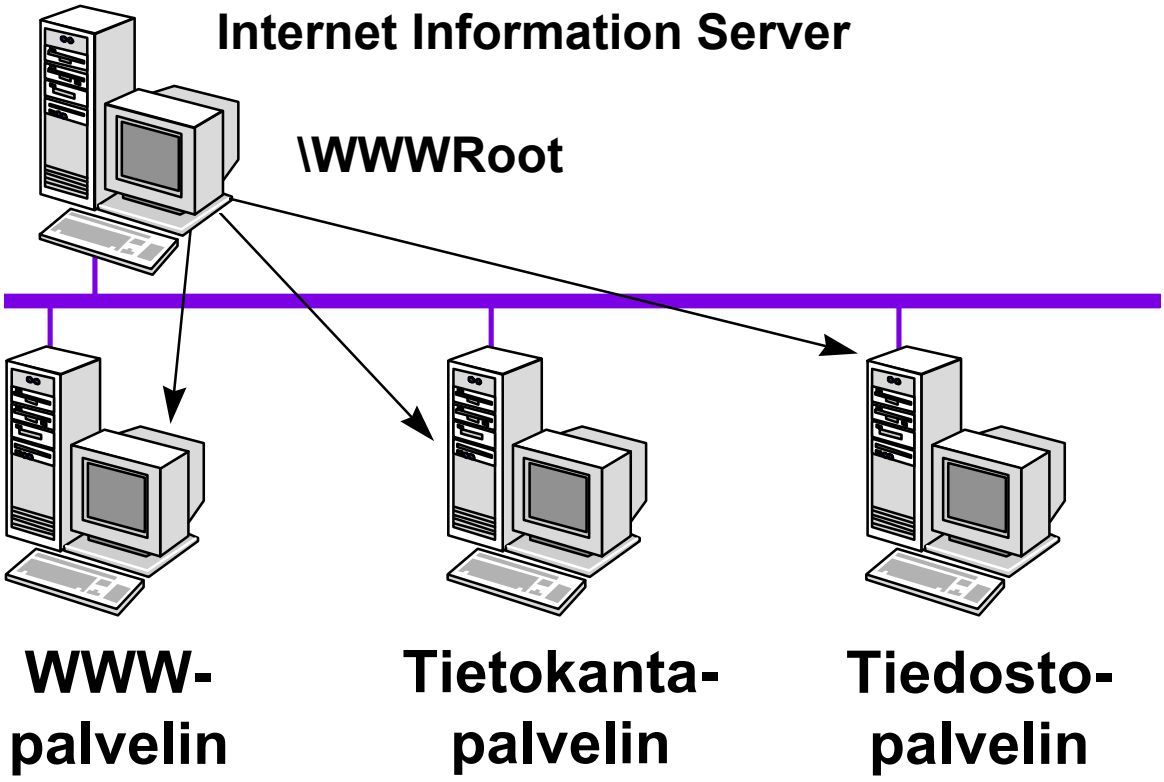
Toisessa esimerkissä hakemistorakenne on jaettu haaroiksi **\PUBLIC** ja **\PRIVATE**. Tämän rakenteen ansiosta valvonta on helppo toteuttaa **\PRIVATE**-hakemistossa ja sen kaikissa alihakemistoissa, kun taas **\PUBLIC**-hakemisto on kaikkien käytettävissä:

Päähakemisto	Alihakemistot	Alihakemistot
\WWWRoot	\PRIVATE	\DATA, \PROGRAMS
	\PUBLIC	\DATA, \PROGRAMS

Kolmannessa esimerkissä hakemistorakenne ei ole monitasoinen. Kotisivu on sijoitettu **\WWWRoot**-hakemistoon, ja kaikki hyperlinkeillä liitetyt sivut ovat alihakemistojen haaroissa. Kussakin alihakemistossa on sivu ja siihen liittyvä grafiikka ja ohjelmat. Joidenkin hakemistojen käyttöä voi olla rajoitettu niin, että ainoastaan työntekijöillä on niiden käyttöoikeus:

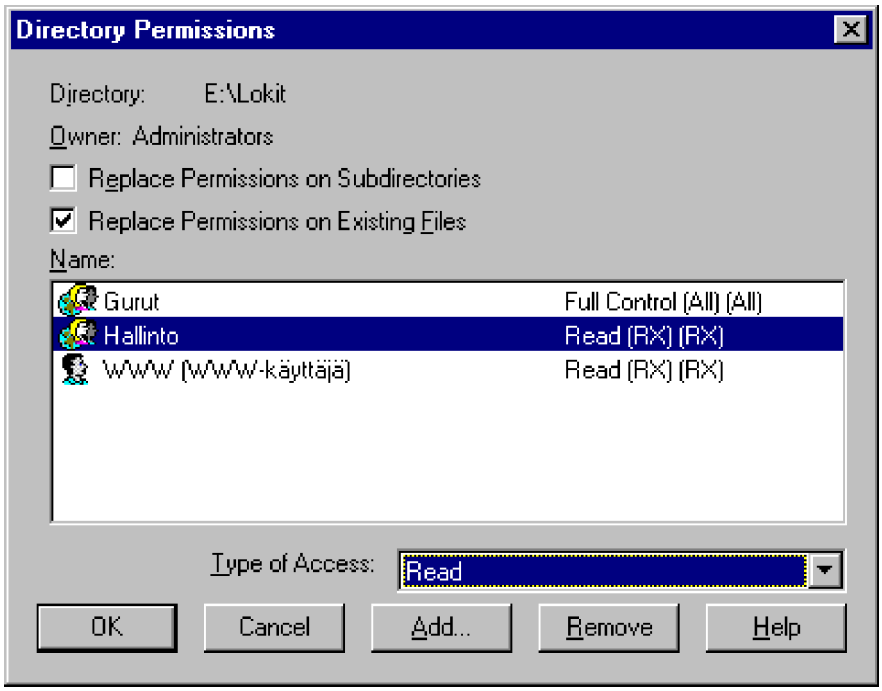
Päähakemisto	Alihakemistot
\WWWRoot	\Yritysesittely
Kotisivu	\Tuotekuvaukset
	\Hinnasto
	\Kontaktit

Viimeisessä esimerkissä hakemistorakenne on levitetty useaan hakemistoon hyödyntämällä Internet Information Serverin virtuaalihakemisto-ominaisuuksia. Virtuaalihakemistojen avulla hakemistoja voidaan sijoittaa toisille palvelimille, joita WWW-asiakkaat voivat käyttää aivan kuin ne olisivat samalla palvelimella:



Hakemiston lisääminen

Uuden kansion voit luoda haluttuun paikkaan hiiren pikavalikosta valitsemalla **New** | **Folder**. Luotuasi uuden hakemiston voit valita kansion sekä valita hiiren pikavalikosta **Properties**, valitse sitten **Security**-välilehti ja lopuksi **Permissions**-painike.



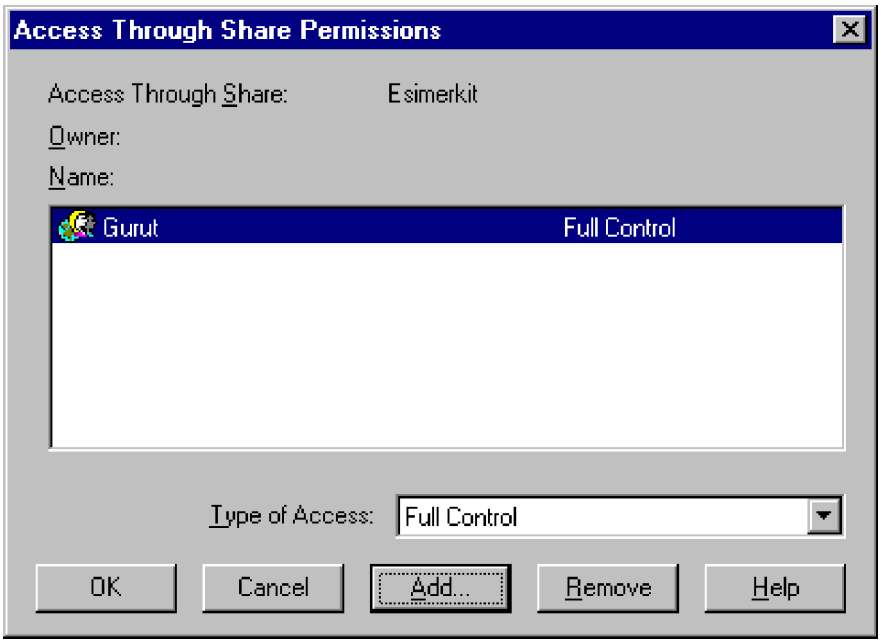
Napauta **Add**-painiketta ja lisää uusi käyttäjä tai ryhmä käyttöoikeuslistaan.

Napauta **Remove**-painiketta, jos haluat poistaa käyttäjän tai ryhmän käyttöoikeuslistasta. Muuta käyttäjätunnuksen oikeuksia napauttamalla sitä ja valitsemalla sitten oikeus **Type of Access** -kentästä.

Voit helpottaa oikeuksien määrittelyä luomalla erityisiä ryhmiä. Esimerkissä on käytetty ryhmää nimeltään **Hallinto**, johon kuuluvat kaikki ne organisaation käyttäjät, joille on annettava vähintään lukuoikeus ja ryhmä **Gurut**, johon kuuluvat ne, jotka tekevät ja lisäävät aineistoa palvelimelle. Ryhmille annetaan riittävät oikeudet haluttuihin hakemistoihin.

Tyypillisesti sisällöstä vastaavien on päästävä suoraan verkon kautta käsiksi kansioihin, joten ne on jaettava verkkoon. Näin he voivat avata kansiot omalta työasemaltaan ja työskennellä suoraan sisällön kanssa.

Valitse kansio ja hiiren pikavalikosta **Properties** ja sitten **Sharing**-välilehti. Valitse **Shared as** -painike ja täytä esiin tuleva lomake sopivalla tavalla.



Jos haluat anonyymien käyttäjien pääsevän hakemistoon, varmista että joko **Guests**-, **Everyone**- tai **IUSR_palvelimennimi**-käyttäjätunnuksilla on hakemistoon lukuoikeudet. Jos taas haluat, että hakemiston käyttöoikeus on vain valtuutetuilla käyttäjillä, poista nämä ryhmät ja käyttäjätunnukset ja lisää sitten käyttäjätunnukset, joilla pitää olla pääsy hakemistoon. Esimerkissä vain ryhmällä **Gurut** on täydet oikeudet verkon kautta hakemistoon.

Kun olet luonut uuden hakemiston, se on määriteltävä Internet Information Serverille käytettävissä olevien hakemistojen listaan. Voit antaa hakemistolle erityisen nimen, jonka avulla käyttäjien on helpompi käyttää sitä.

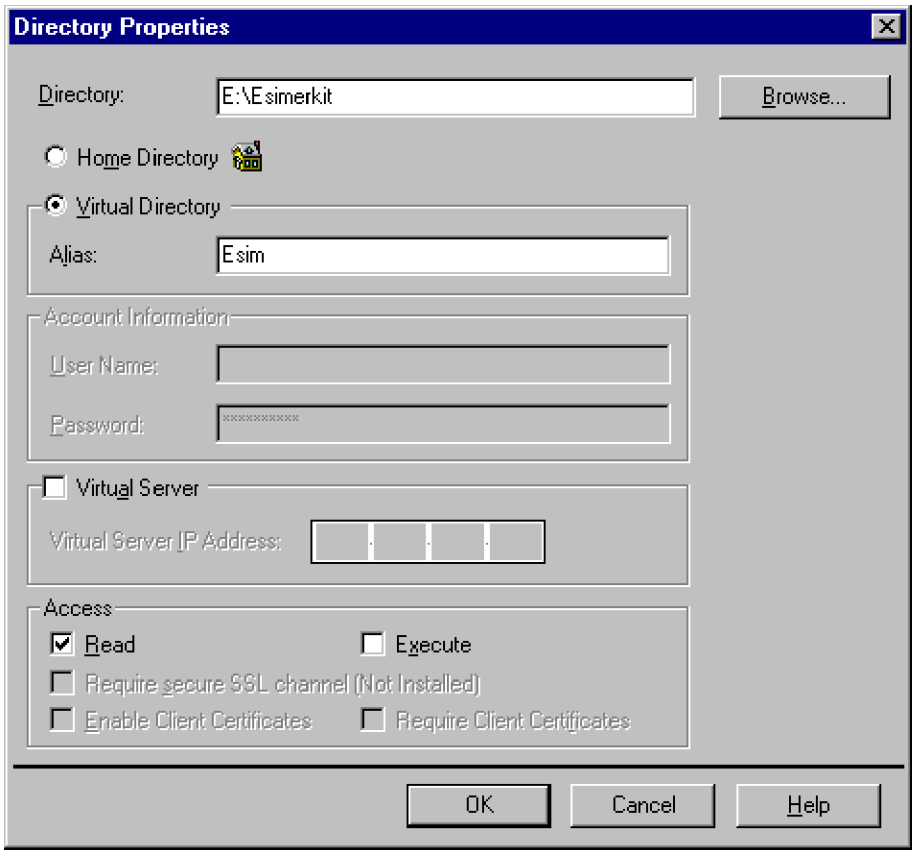
Tämä tehdään seuraavasti:

1) Avaamalla Internet Service Manager ja kaksoisnapauta sitä WWW-palvelinta, jonka kanssa haluat työskennellä. Kun **Properties**-valintaikkuna aukeaa, valitse **Directories**-välilehti

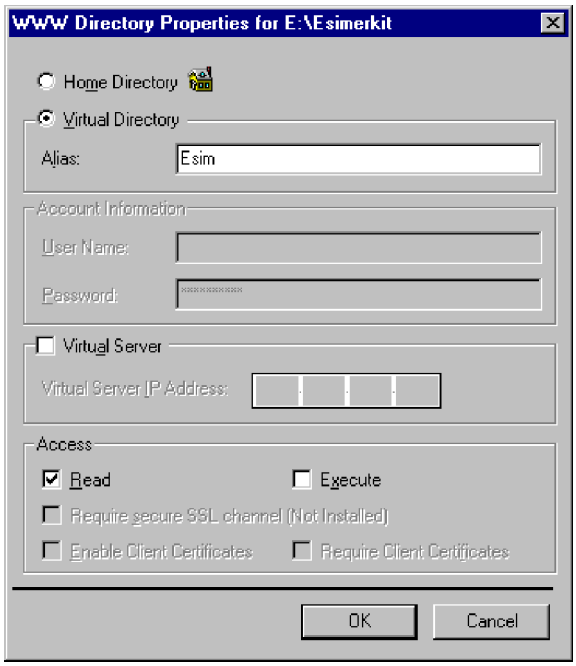
2) Esiin tulee lista, jossa näkyvät nykyiset hakemistot. Voit tehdä jommankumman seuraavista toimista:

- Kaksoisnapauta olemassa olevaa hakemistoa, jolloin sen **Directory Properties** -valintaikkuna aukeaa
- Lisää uusi hakemisto napauttamalla **Add**-painiketta.

3) Voit etsiä hakemistoa hakemistopuusta valitsemalla **Browse**-painikkeen. Kun olet löytänyt haluamasi hakemiston, sen nimi näkyy **Directory**-kentässä.

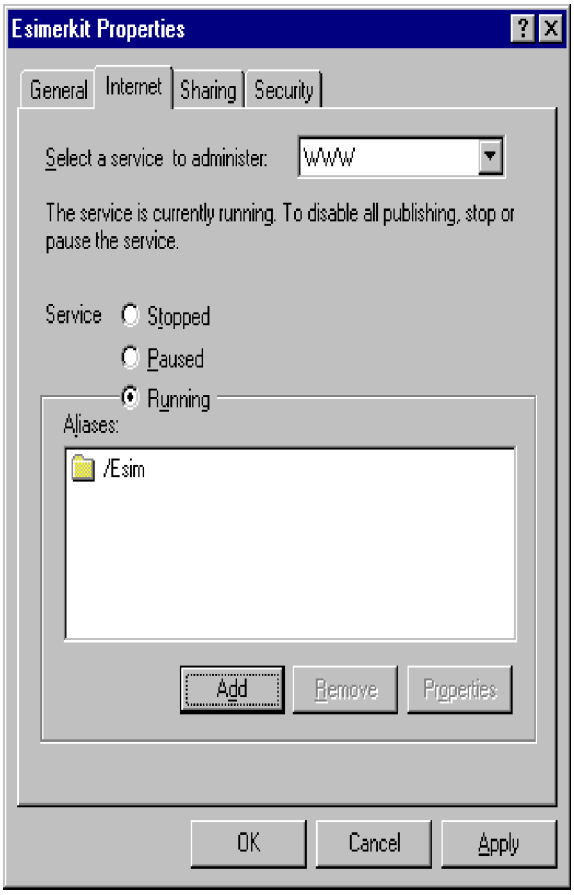


Toinen tapa tehdä sama on valita kansio Resurssienhallinnalla (Explorer) ja valita hiiren pikavalikosta **Properties**. Jos olet asentanut kyseiseen palvelimeen **IIS**:n, käytettävissäsi on **Internet**-välilehti:



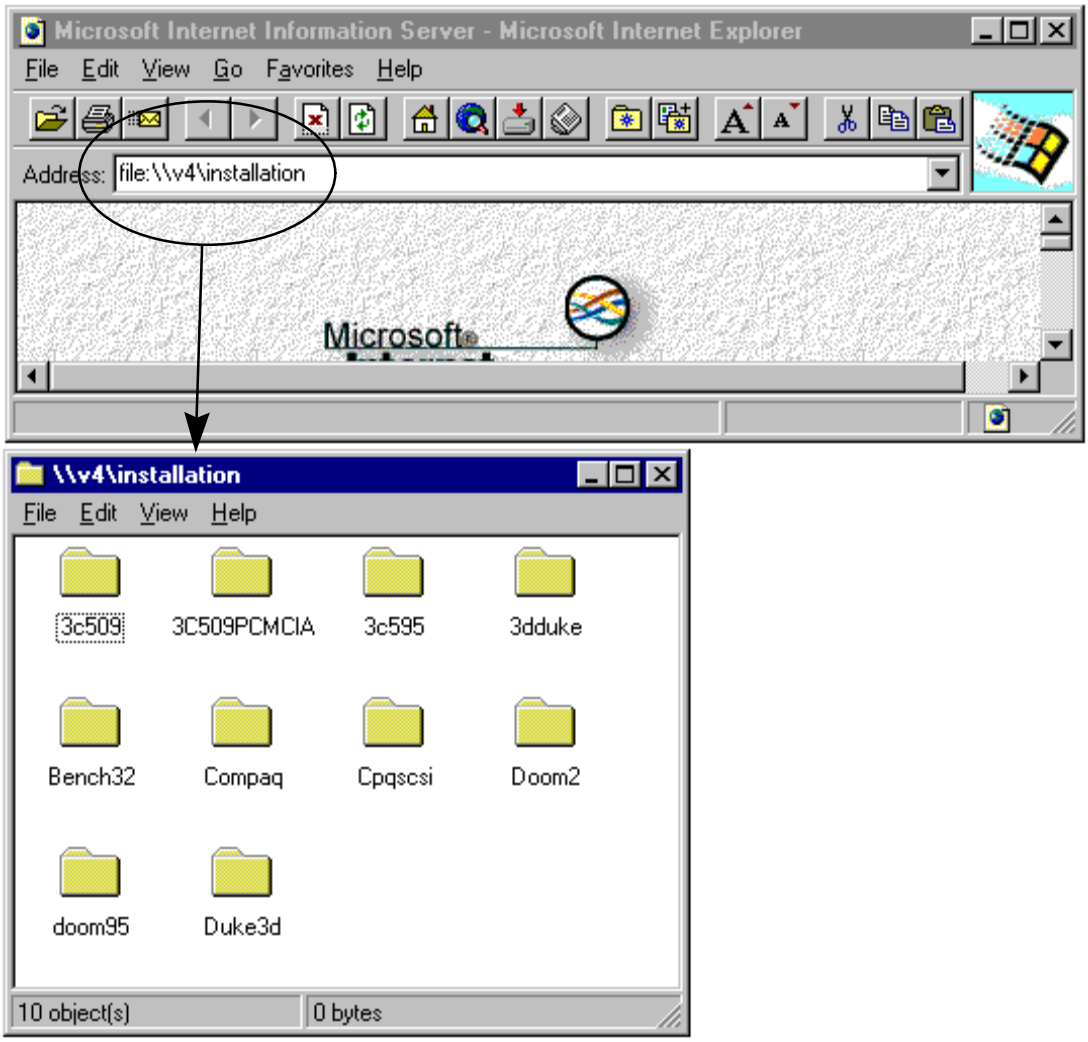
Tässä asetukset ovat aivan samat kuin määriteltäessä hakemisto IIS:n kautta.

Kun hakemisto on määritelty, se näkyy myös **Internet**-välilehdessä:

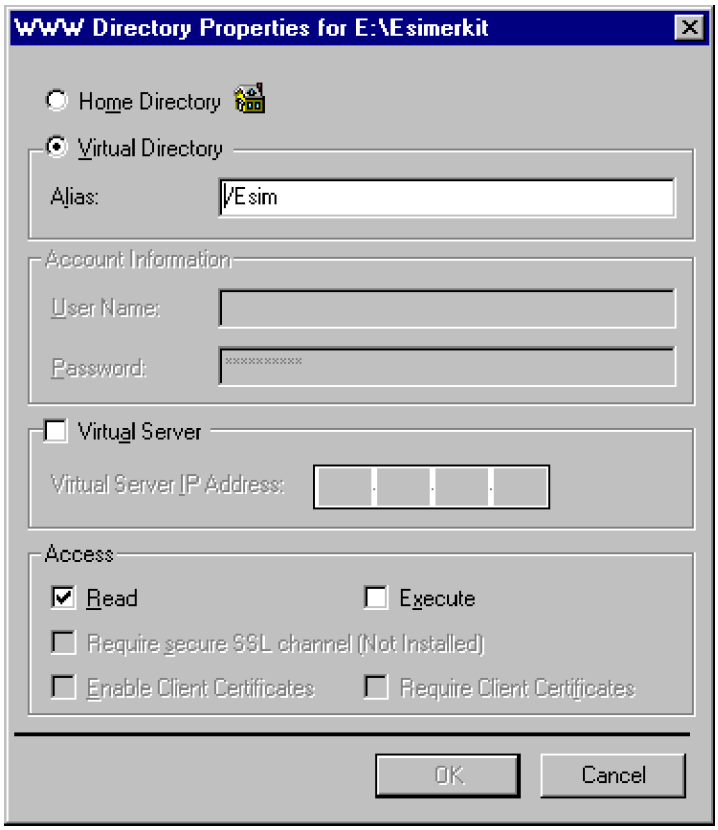


Hakemiston lisääminen **Service Properties** -valintaikkunaan ei ole ainoa tapa antaa WWW-käyttäjille hakemiston käyttöoikeutta.

Käyttäjät voivat edelleenkin käyttää kaikkia niitä hakemistoja, joihin heille annettu luku- tai suoritusoikeus kirjoittamalla hakemiston UNC-nimen WWW-selaimensa URL-osoitekenttään, esimerkiksi **\\V4\Installation**.



Hakemiston konfigurointi



Directory Properties -sivulla tai **Internet**-välilehdessä voit tehdä seuraavat asetukset:

- **Home Directory** - jos valitsemasi hakemisto on WWW-palvelimen päähakemisto, jonne kotisivu on tallennettu, valitse **Home Directory** -valintanappi. Jos **Enable Default Directory** -valintaruutu **Directory**-sivulla on valittu, tämän hakemiston HTML-oletussivu näytetään, kun käyttäjät avaavat kotisivun

- **Virtual Directory** - valitse **Virtual Directory** -valintanappi, kun haluat määritellä aliasnimen samalla levyasemalla, toisella levyasemalla tai toisella palvelimella olevalle hakemistolle. Aliasnimi on yksinkertaisesti nimi, jota WWW-asiakas käyttää siirtyessään hakemistoon, ilman että se kertoo mitään hakemiston todellisesta sijaintipaikasta. Jos esimerkiksi **FishWaren** WWW-sivuilla hakemisto on fyysisesti eri palvelimella ja sen aliasnimi on **/Feeder**, asiakas voi päästä sinne URL-osoitteella **http://www.fishware.fi/Feeder**

- **Account Information** - jos annoit toisella palvelimella sijaitsevan hakemiston nimen, **Account Information** -ryhmä on aktiivinen. Kirjoita kenttiin **käyttäjätunnus** ja **salasana**, joita vaaditaan ennen kuin levyasemaan päästään käyttäjäksi. Verkkoasemilla olevien virtuaalihakemistojen on oltava Internet Information Serverin kanssa samaan Windows NT -toimialueeseen kuuluvilla NT-koneilla. Kaikki hakemiston käsittely tapahtuu määrittelemäsi käyttäjätunnuksen ja salasanan kautta. Muista, että tällä käyttäjätunnuksella käyttäjät pääsevät toiseen järjestelmään, joten käyttäjätunnuksella tulisi olla kohdekoneessa vain minimioikeudet!

- **Virtual Server** - yksi Internet Information Server -palvelin voi isännöidä useita toimialueita, esim. **http://www.fishware.fi** ja **http://www.frogware.fi**. WWW-käyttäjillä voi olla pääsy kumpaankin toimialueeseen tietämättä, että ne ovat samalla palvelimella. Kirjoita **Virtual Server** -kenttään IP-osoite, johon virtuaalipalvelin viittaa

- **Access** - tässä ryhmässä on ne oikeudet, joita anonyymeillä käyttäjillä on tässä hakemistossa. Huomaa, että näillä asetuksilla suojataan ensisijaisesti **muita** kuin NTFS-hakemistoja. NTFS-hakemistojen suojausasetukset voidaan tehdä hakemiston **Permissions**-valintaikkunassa.

Hakemiston käyttöoikeudet

Kun olet lisännyt uuden hakemiston, johon käyttäjät voivat päästä WWW-palvelimen kautta, sinun on määriteltävä, millaisia **käyttöoikeuksia** käyttäjillä hakemistossa on. Oikeuksia on kolmea tyyppiä:

- **Read** - eli lukuoikeudet sallivat käyttäjien katsella hakemiston tiedostoja, mutta he eivät voi itse muuttaa tai lisätä tiedostoja. Tämä vaihtoehto on turvallisin - esimerkiksi WWW-sivuja sisältävässä hakemistossa voidaan ottaa lukuoikeus käyttöön, mutta ohjelmia sisältävässä hakemistossa sen voi ottaa pois käytöstä, jotta asiakassovellukset eivät voi kopioida ohjelmiasi

- **Execute** - suoritusoikeuksilla käyttäjät voivat käynnistää hakemistossa olevia sovelluksia tai skriptejä. Asiakkaan pyyntö saattaa suorittaa **CGI**- tai **ISAPI**-sovelluksen, kun selaimen

URL-osoitekenttään kirjoitetaan sovelluksen tiedostonimi. Voit käyttää myös **Web File Extension Mapping** -ominaisuutta, jonka avulla ajettavat ohjelmat ja DLL-kirjastot voidaan tallentaa muualle kuin WWW-aineiston kanssa samaan hakemistopuuhun. Web File Extension Mappingia käytetään paikantamaan tiedosto paikalliselta WWW-palvelimelta tai toiselta WWW-palvelimelta

- **Require Secure SSL Channel** - vaaditaan SSL-yhteys. Kun **Secure Sockets Layer** on asennettu, **Require Secure SSL Channel** -valinta on käytettävissä, ja sen avulla voidaan lähettää salatusti hakemistossa olevaa tietoa asiakkaalle. Kun tämä valinta on käytössä, asiakkaan ja palvelimen välillä käytetään suojattua ja salakirjoittavaa kanavaa.

Huomattavaa:

- **Internet Information Serverin** asennuksen yhteydessä luodaan **\Scripts**-niminen hakemisto. Tällä hakemistolla on suoritusoikeus (eikä lukuoikeutta), ja se on IIS:n päähakemiston alihakemisto. Kaikki **Internet Server API** (ISAPI) -sovellukset ja **Common Gateway Interface** (CGI) -skriptit pitäisi tallentaa tähän hakemistoon tai luoda skriptien tallennukseen toinen hakemisto, jolla on sanat suoritusoikeudet

- Älä anna kirjoitusoikeuksia hakemistoihin, joissa on **suoritettavia skriptejä**. Krakkerit voivat siirtää hakemistoon järjestelmääsi vahingoittavia ohjelmia ja suorittaa niitä siellä

- **Directory Properties** -valintaikkunassa olevien käyttöoikeuksien on oltava samat kuin hakemiston **NTFS**-asetuksissa

- Tietokantoja sisältävillä hakemistoilla on syytä olla **kirjoitusoikeus** (Write), mutta ei **suoritusoikeutta** (Execute). Jos krakkeri onnistuisi siirtämään ikävän ohjelman hakemistoon, sitä ei kuitenkaan voida ajaa, koska hakemistolla ei ole tällöin tarvittavaa suoritusoikeutta.

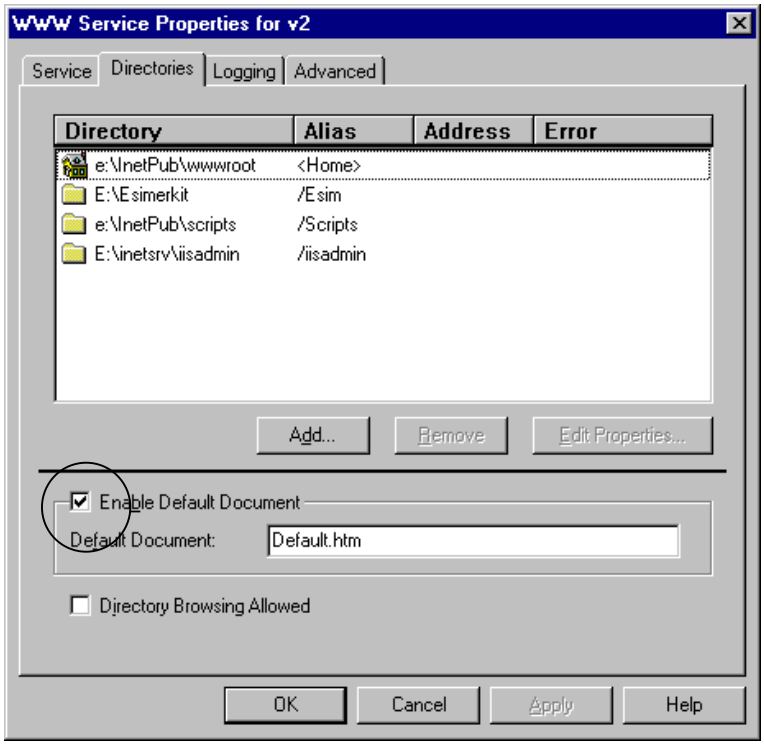
Ehdotuksia hakemistojen oikeuksista NTFS-levyillä:

Hakemiston sisältö	Kuvaus	NTFS-oikeudet
WWW-sisältöä	WWW-sivut ja -kuvat	Luku (Read)
Scriptejä	Sisältää suoritettavia ohjelmia ja skriptejä	Suoritus (Execute)
Tietokanta	Sisältää tietokantoja	Read (Luku) ja kirjoitus (Write)

Oletussivut

Kun WWW-käyttäjät tulevat WWW-sivulle, he saattavat antaa URL-perus-osoitteen (esim. **http://www.fishware.fi**) tai osoitteen, jossa on mainittu jokin tietty hakemisto ja HTML-tiedosto (esim. **http://www.fishware.fi/feeder.htm**).

Oletussivut otetaan käyttöön avaamalla **Directory Properties** -sivu ja valitsemalla **Enable Default Document** -kenttä.

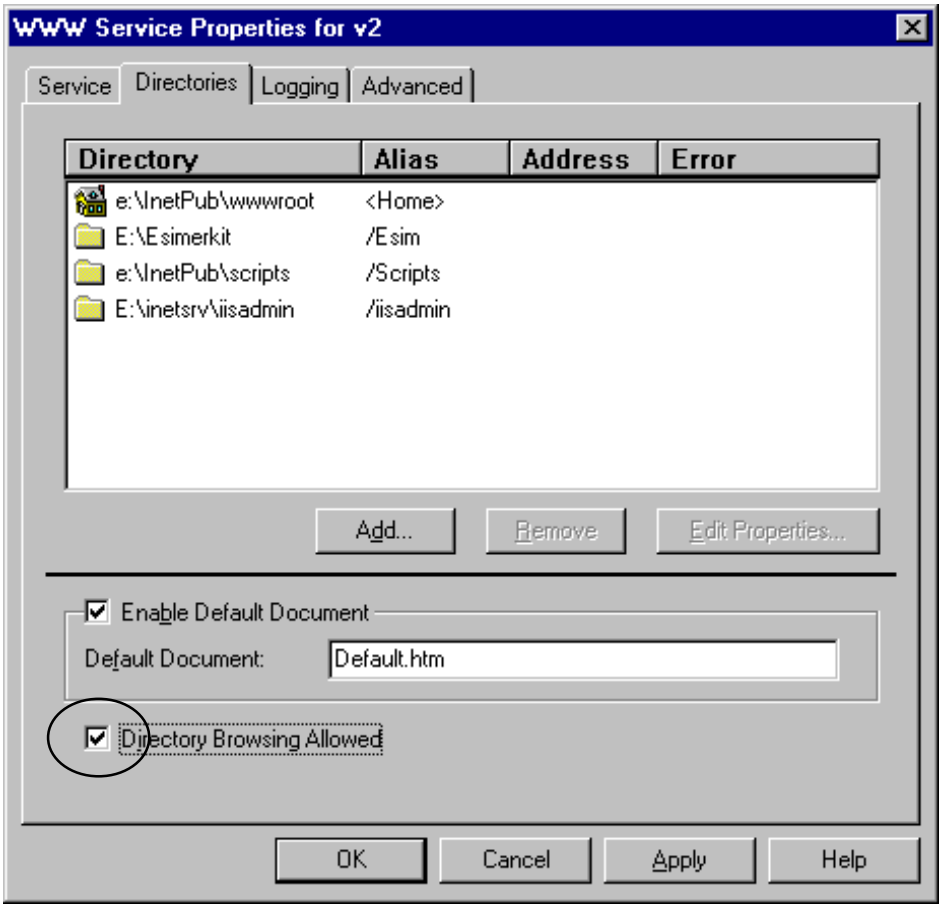


Varmista, että kirjoitat **Default Document** -kenttään tiedostonimen. Oletuksena tiedostonimi on **Default.htm**, mutta voit muuttaa sitä. Sen jälkeen (tai ennen) voit luoda hakemistoon tämän nimisen HTML-sivun.

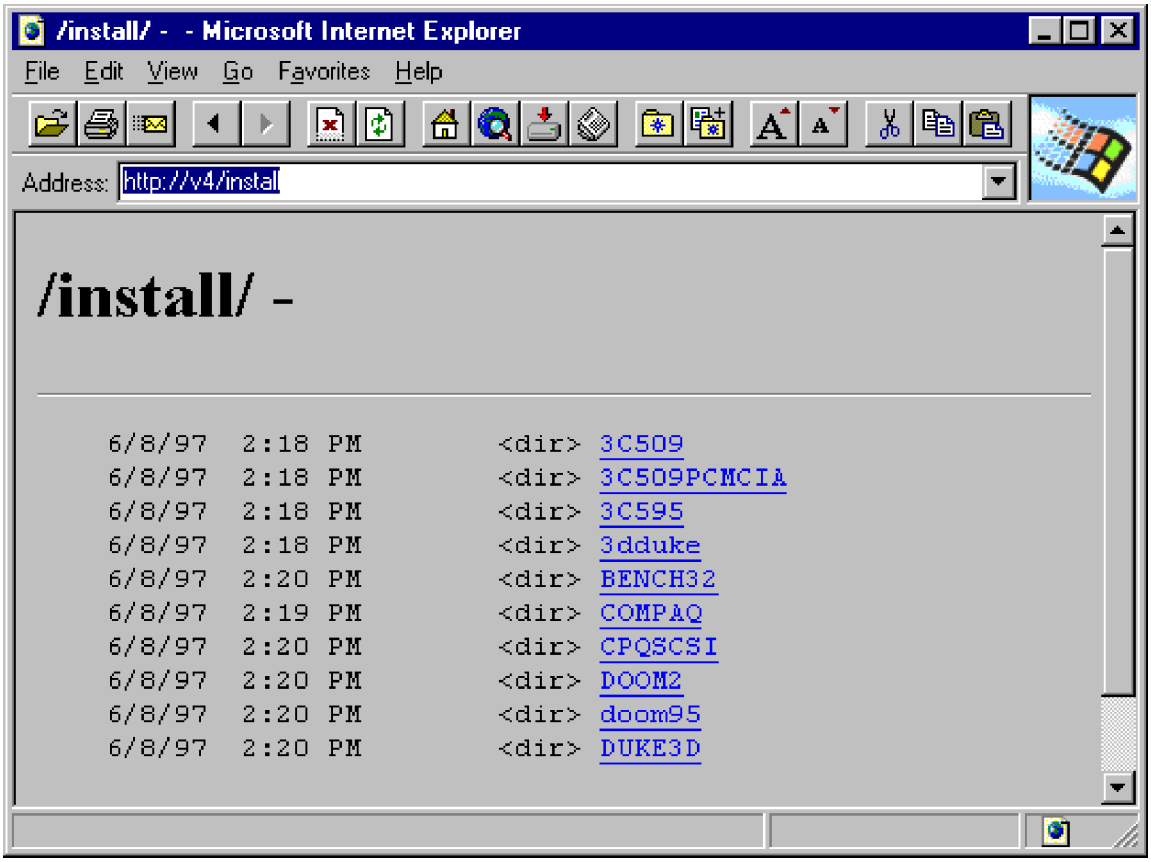
Jos hakemistossa ei ole oletussivua jatko riippuu siitä, mitä WWW-palvelimen **hakemistoselausvalinnassa** (*Directory Browsing*) on määritelty.

Hakemistoselaus

Hakemistoselaus otetaan käyttöön **Directory Properties** -sivun **Directory Browsing Allowed** -valinnalla.



Kun se on käytössä, käyttäjä näkee tiedostolistan avatessaan hakemiston, jossa ei ole oletussivua.



Hakemistoselausta käytettäessä WWW-palvelimesi näyttää FTP-palvelimelta, jossa käyttäjät voivat siirtää tiedostoja suoraan omaan järjestelmäänsä. He voivat vetää ja pudottaa (*Drag and drop*) tiedostoja työpöydälleen tai käyttää hiiren pikavalikkoa ja tarkastella käytettävissä olevia vaihtoehtoja. Tämä voi olla kätevää silloin, kun halutaan jakaa tiedostoja.

Jos hakemistoselaus on mielestäsi tietoturvallisuutta uhkaava menetelmä tapa jakaa tietoa, voit jättää ottamatta ominaisuuden käyttöön. Silloin käyttäjät näkevät virheilmoituksen yrittäessään siirtyä suojattuun hakemistoon.

Virtuaalihakemistot eivät näy hakemistoselausta käytettäessä.

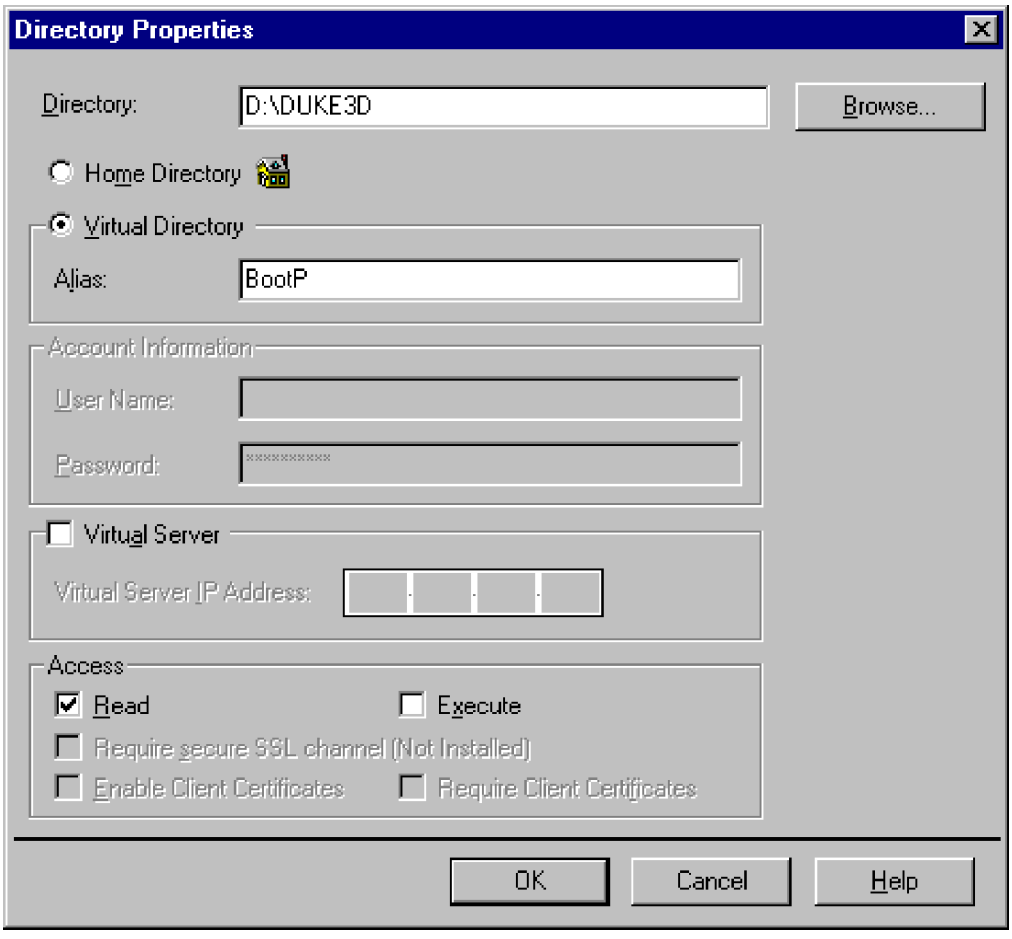
Virtuaalihakemistot

Virtuaalihakemisto tarkoittaa menetelmää, jossa hakemiston nimi sinänsä ei näy WWW-asiakkaalle. Nimi voi olla lähes mitä tahansa, ja virtuaalihakemisto voi jopa osoittaa toiseen palvelimeen.

Paikallinen virtuaalihakemisto luodaan seuraavasti:

1) Avaa Internet Service Manager ja kaksoisnapauta sitä WWW-palvelinta, jonka kanssa haluat työskennellä. Kun **Properties**-valintaikkuna aukeaa, valitse **Directories**-välilehti

2) Esiin tulee lista, jossa näkyvät nykyiset hakemistot. Lisää uusi hakemisto napauttamalla **Add**-painiketta

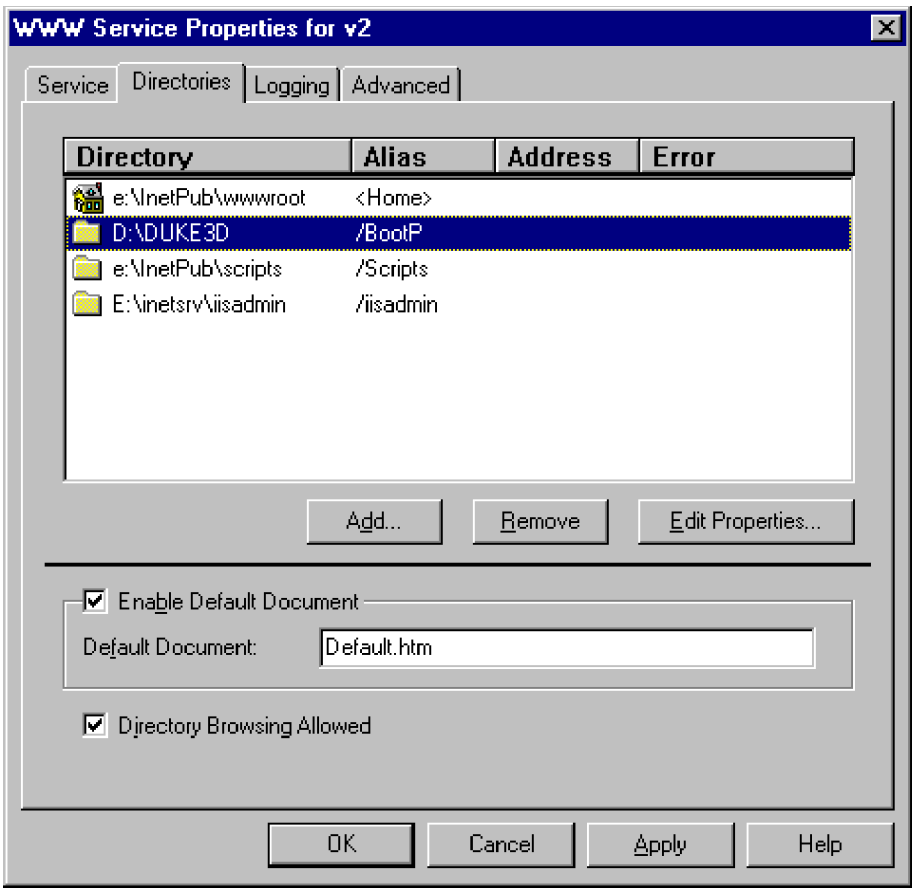


3) Voit etsiä hakemistoa hakemistopuusta valitsemalla **Browse**-painikkeen. Kun olet löytänyt haluamasi hakemiston, sen nimi näkyy **Directory**-kentässä

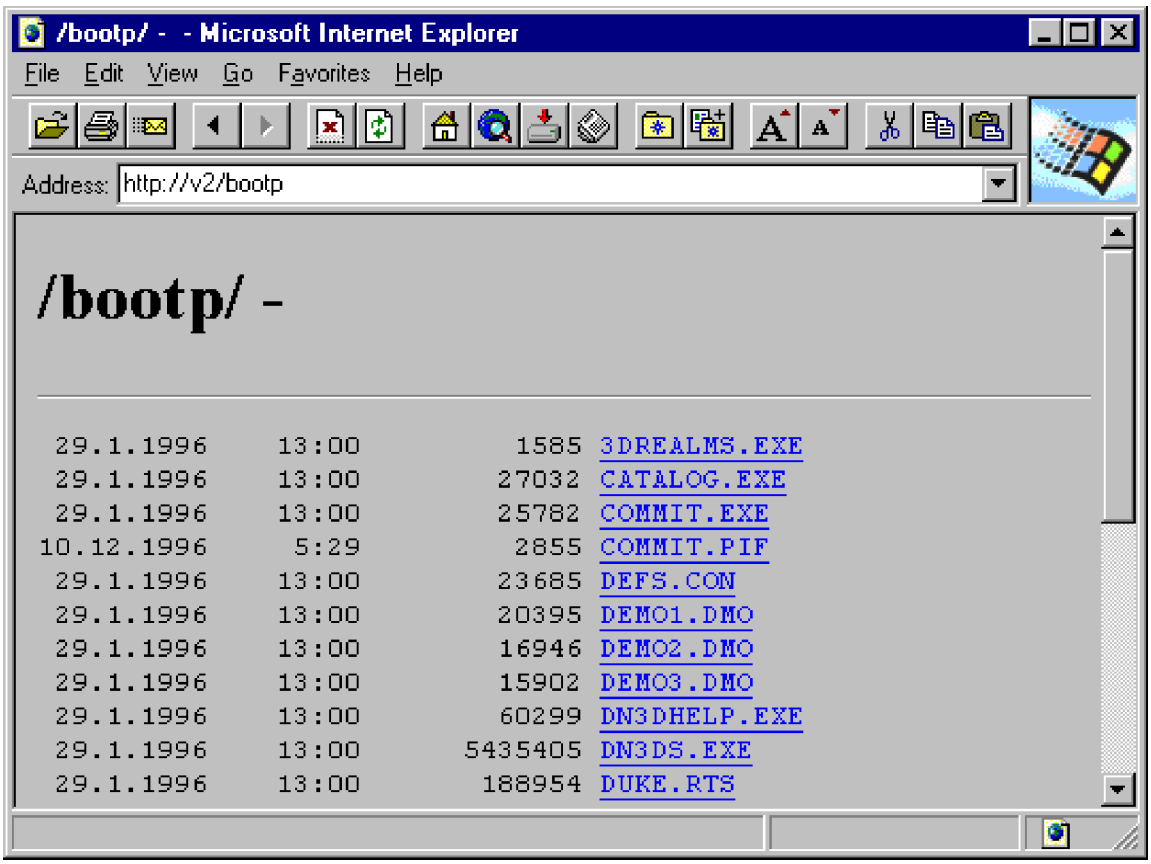
4) Valitse **Virtual Directory** ja anna haluamasi **Alias**

5) Anna tarvittaessa käyttöoikeudet (**Access**) ja paina **OK**

6) Virtuaalihakemisto tulee näkyviin WWW-palvelimen hakemistojen luetteloon.



Tämän jälkeen hakemistoon pääsee antamalla virtuaalihakemiston aliasnimi:

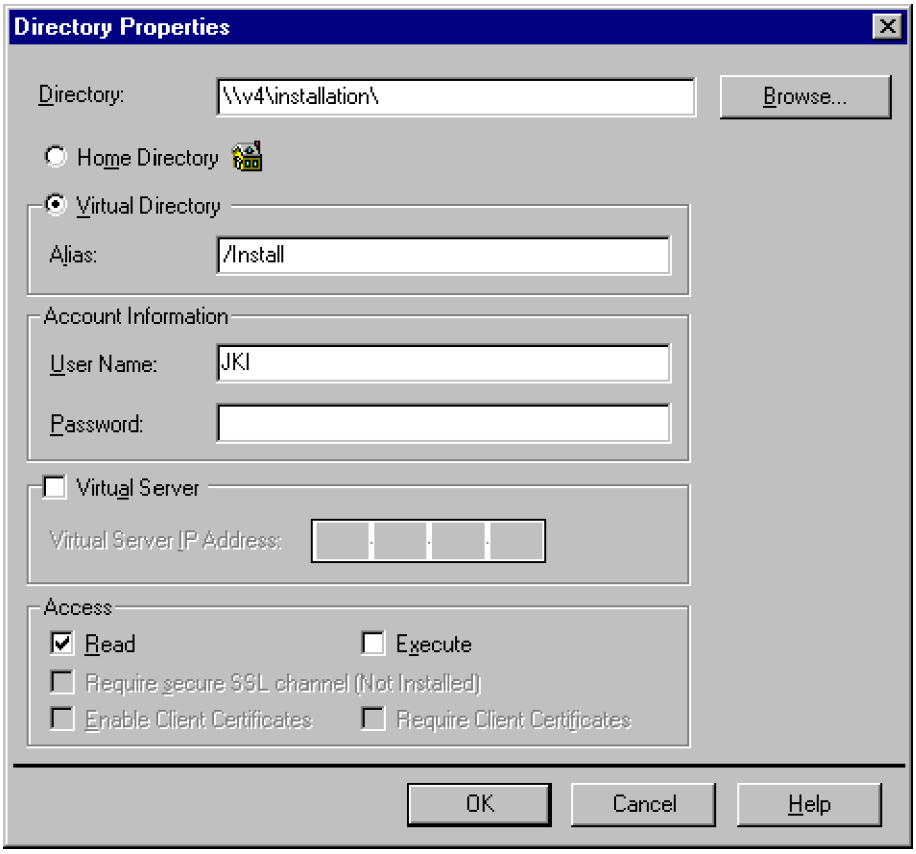


Virtuaalihakemisto voi sijaita myös toisessa palvelimessa. Tällainen virtuaalihakemisto määritellään seuraavasti:

1) Avaa Internet Service Manager ja kaksoisnapauta sitä WWW-palvelinta, jonka kanssa haluat työskennellä. Kun **Properties**-valintaikkuna aukeaa, valitse **Directories**-välilehti

2) Esiin tulee lista, jossa näkyvät nykyiset hakemistot. Lisää uusi hakemisto napauttamalla **Add**-painiketta

3) Anna hakemiston **UNC-polku Directory**-kenttään

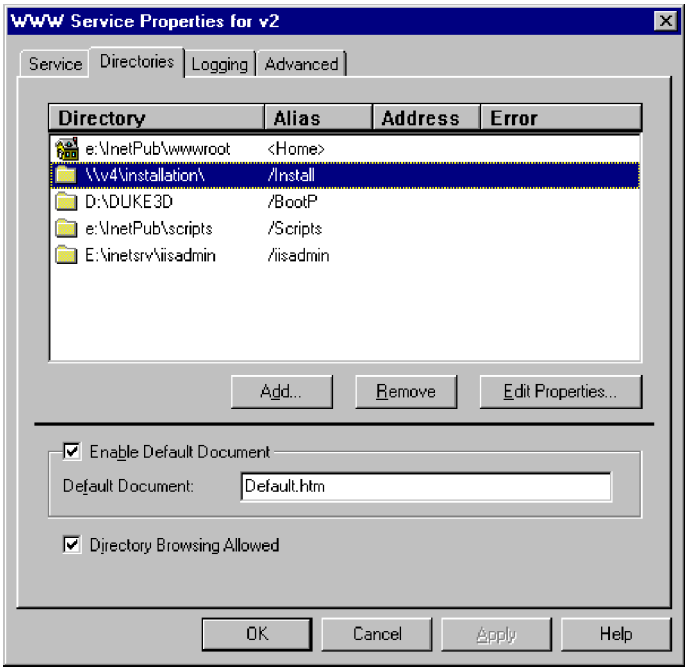


4) Valitse **Virtual Directory** ja anna haluamasi **Alias**

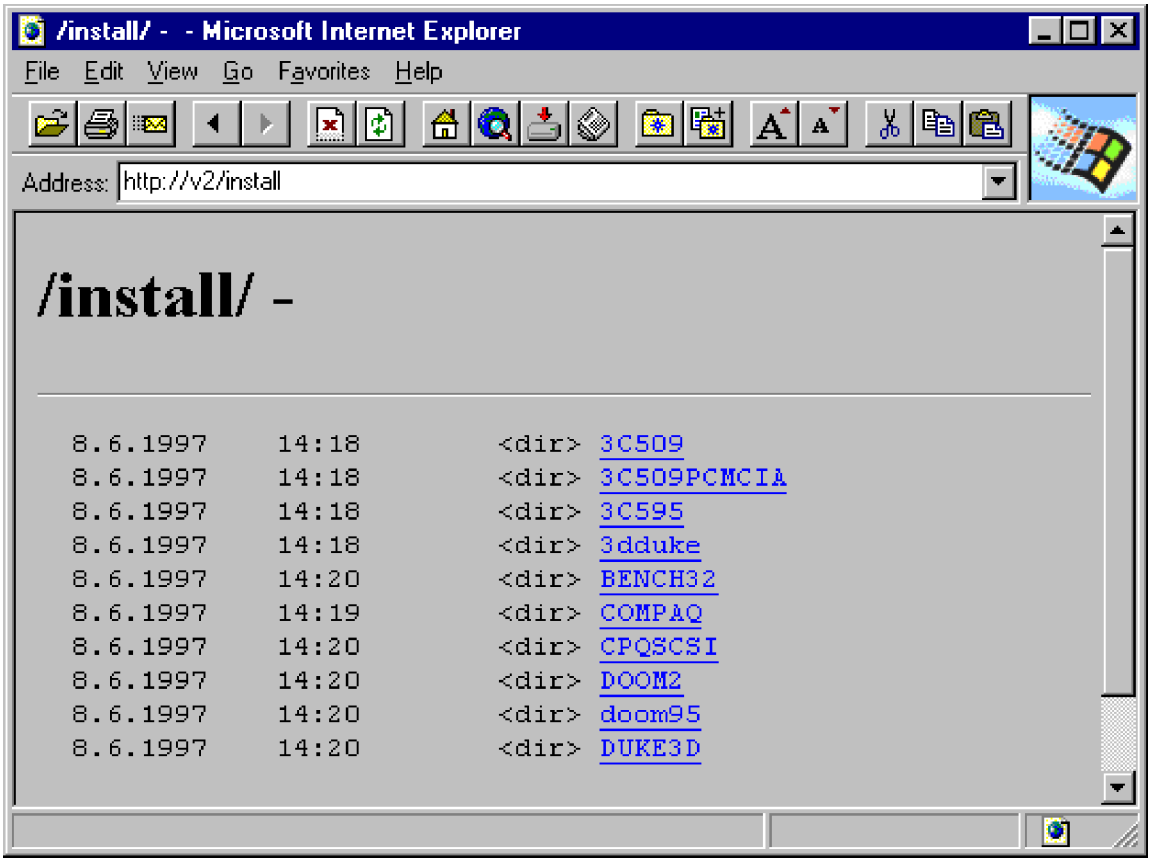
5) Anna tarvittaessa **käyttäjätunnus** (**Account Information**) ja **salasana**, jolla hakemistoon pääsee käyttäjäksi

6) Anna tarvittaessa käyttöoikeudet (**Access**) ja paina **OK**

7) Virtuaalihakemisto tulee näkyviin WWW-palvelimen hakemistojen luetteloon.



Tämän jälkeen hakemistoon pääsee antamalla virtuaalihakemiston aliasnimi:



Virtuaalipalvelimet

WWW-virtuaalipalvelin tarkoittaa menetelmää, jossa rekisteröidään useita IP-osoitteita ja nimiä samaan palvelimeen, esimerkiksi **www.fish-ware.fi** ja **www.penguin.fi**. Tällöin tulee määritellä useampi IP-osoite samaan palvelimeen. Se taas tehdään TCP/IP-asetuksissa valitsemalla **Advanced TCP/IP Configuration**.

Voit myös määritellä nämä eri nimet ja IP-osoitteet nimipalvelussa.

Nimipalvelu voi olla:

- **DNS**-palvelimessa määritelty nimi (esimerkiksi www.toimialue.-fi)
- **HOSTS**-tiedostossa määritelty nimi (esimerkiksi www.toimi-alue.fi)
- **NetBIOS-nimi** (Computername, esimerkiksi SERVERI5)
- **LMHOSTS**-tiedostossa määritelty nimi (esimerkiksi VEPPI).

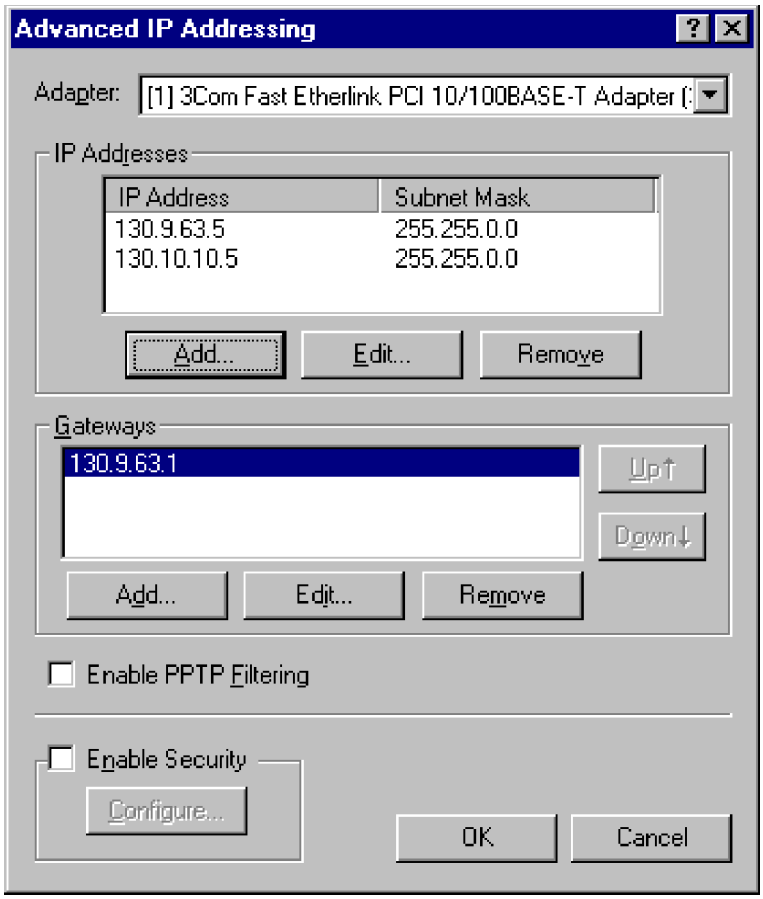
Virtuaalipalvelimen hakemisto voi olla:

- Mikä tahansa IIS-palvelimen paikallinen hakemisto, esimerkiksi **D:\Data**
- Mikä tahansa IIS-palvelimen näkemä levyasema, esimerkiksi **C:** ... **Z:**
- Mikä tahansa UNC-osoite, esimerkiksi **\\SERVERI5\DATA**.

WWW-virtuaalipalvelimen luomisen vaiheet ovat seuraavat:

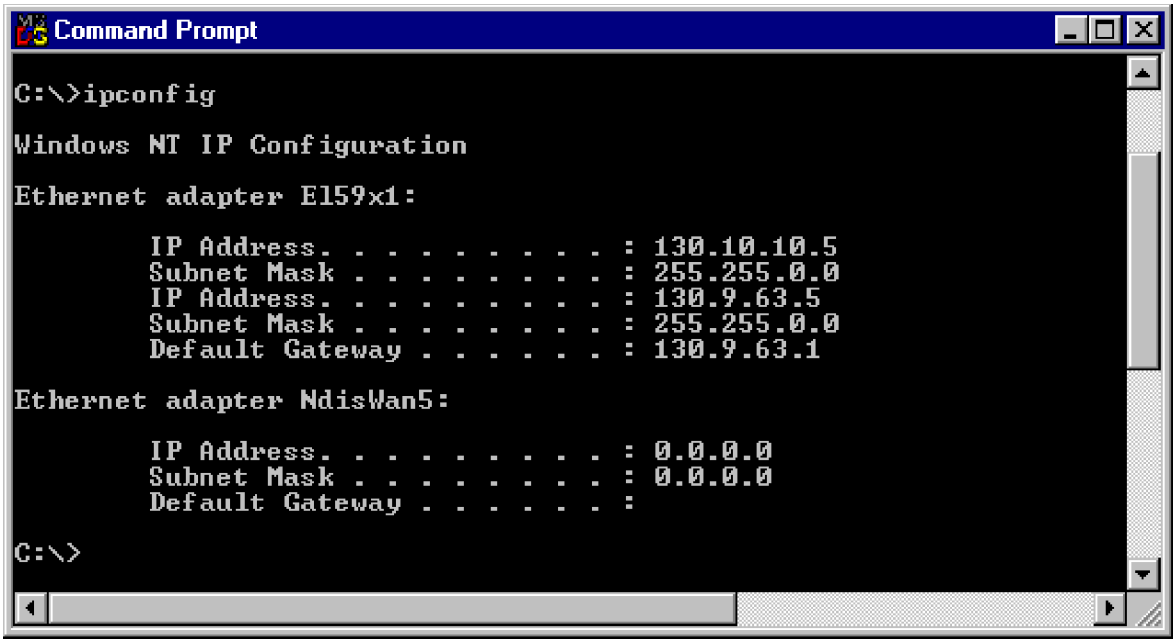
1) Määritä virtuaalipalvelimen **IP-osoite** Ohjauspaneelista **Networkin** avulla valitsemalla **Protocols**-välilehti ja **TCP/IP Protocol**, josta valitaan **Properties**. Valitse **IP Address**-välilehden **Advanced...**

2) Lisää **Add**-painikkeella uusi IP-osoite, anna myös **aliverkon peitto** (Subnet mask) ja paina **OK**



3) Käynnistä palvelin uudelleen, jotta osoite tulee voimaan.

Komentorivin komennolla **IPCONFIG** IP-osoitteiden tulisi näkyä:



Seuraavaksi määritellään virtuaalipalvelin:

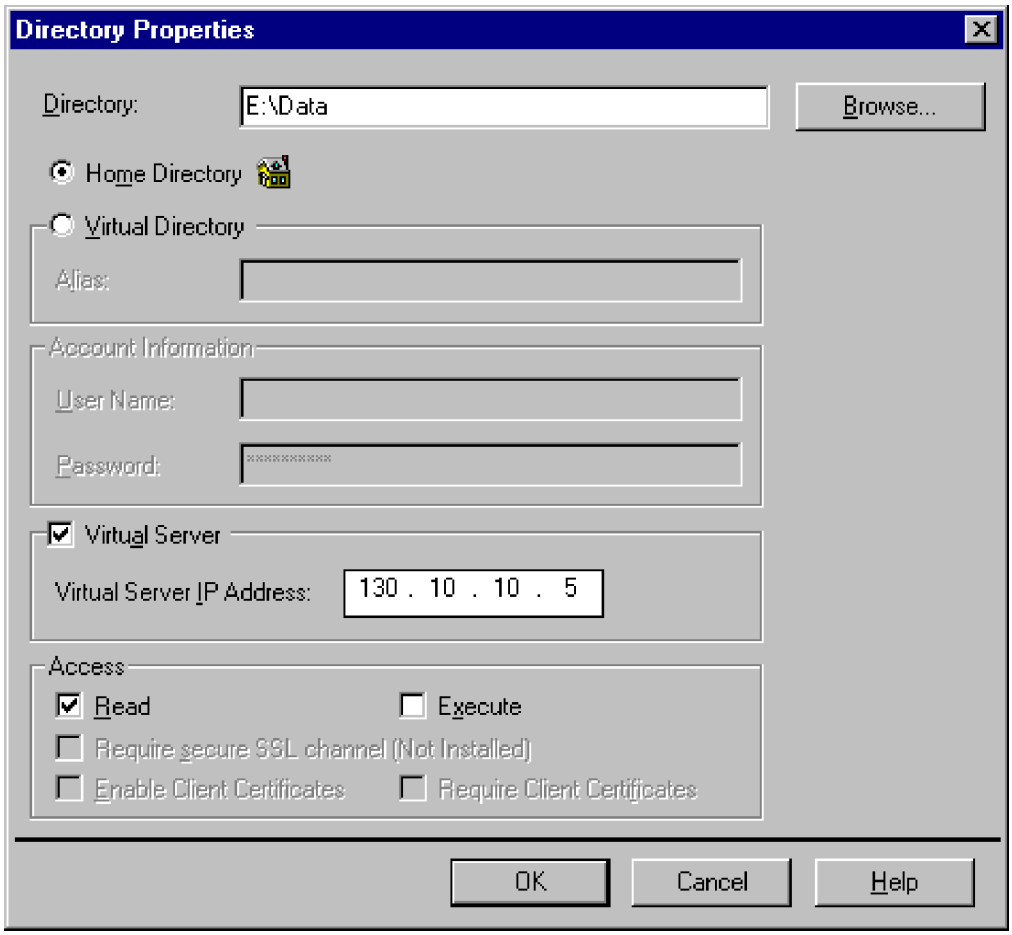
1) Avaa Internet Service Manager, kaksoisnapauta haluttua WWW-palvelinta, ja valitse **Directories**-välilehti

2) Lisää uusi hakemisto napauttamalla **Add**-painiketta

3) Anna tai selaa hakemisto **Directory**-kenttään

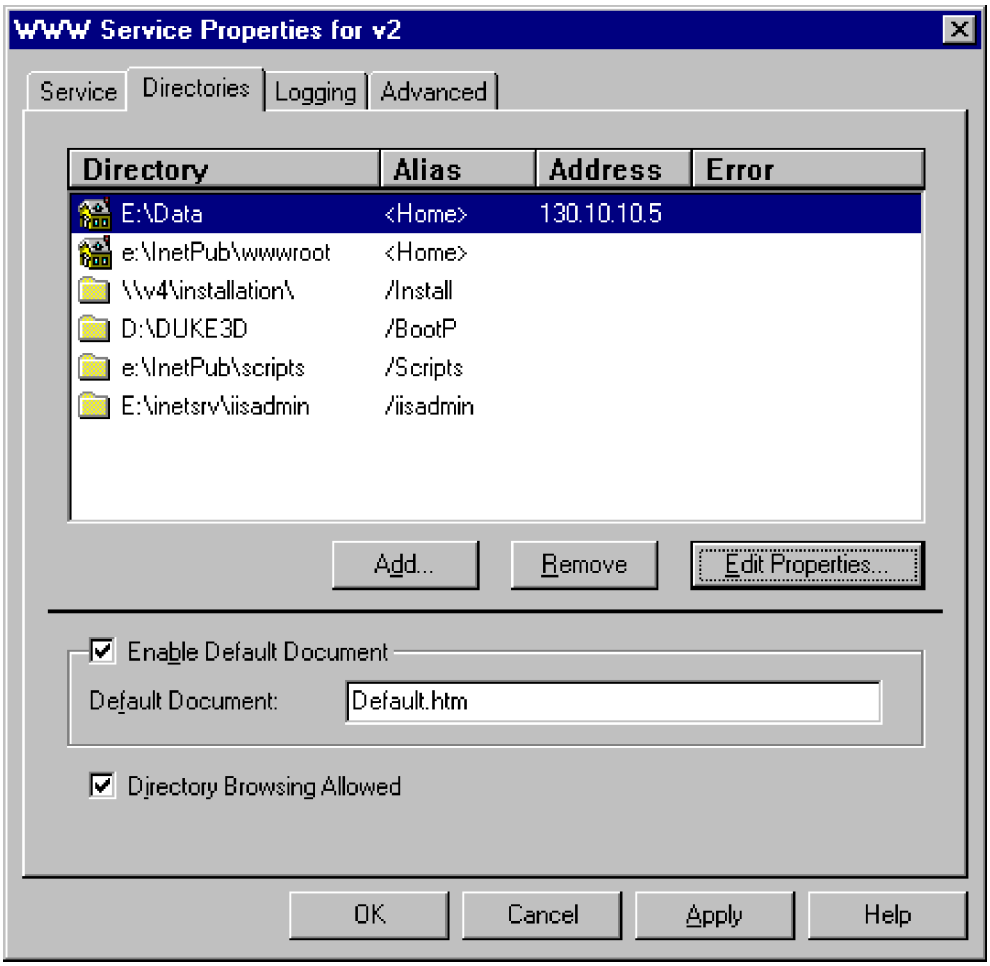
4) Valitse **Home Directory**

5) Valitse **Virtual Server** ja anna **Virtual Server IP Address**-ruutuun äsken määritelty **IP-osoite**



6) Anna tarvittaessa käyttöoikeudet (**Access**) ja paina **OK**

7) Virtuaalihakemisto tulee näkyviin WWW-palvelimen hakemistojen luetteloon.



Jos et ole konfiguroinut nimipalveluja, voit kokeilla suoraan vaikka palvelimella virtuaalipalvelimen toimintaa.

Tee **WINNT\SYSTEM32\ DRIVERS\ETC**-hakemistoon seuraavat tiedostot tai tee olemassaoleviin isäntätiedostoihin tarpeelliset lisäykset oman ympäristösi mukaan - idea on lisätä virtuaalipalvelimen nimi ja IP-osoite (sekä varmuuden vuoksi alkuperäisen IIS-palvelimen nimi ja IP-osoite):

HOSTS-tiedoston asetukset:

```
130.10.10.5     www.fishware.fi
130.9.63.5      v2.fishware.fi
```

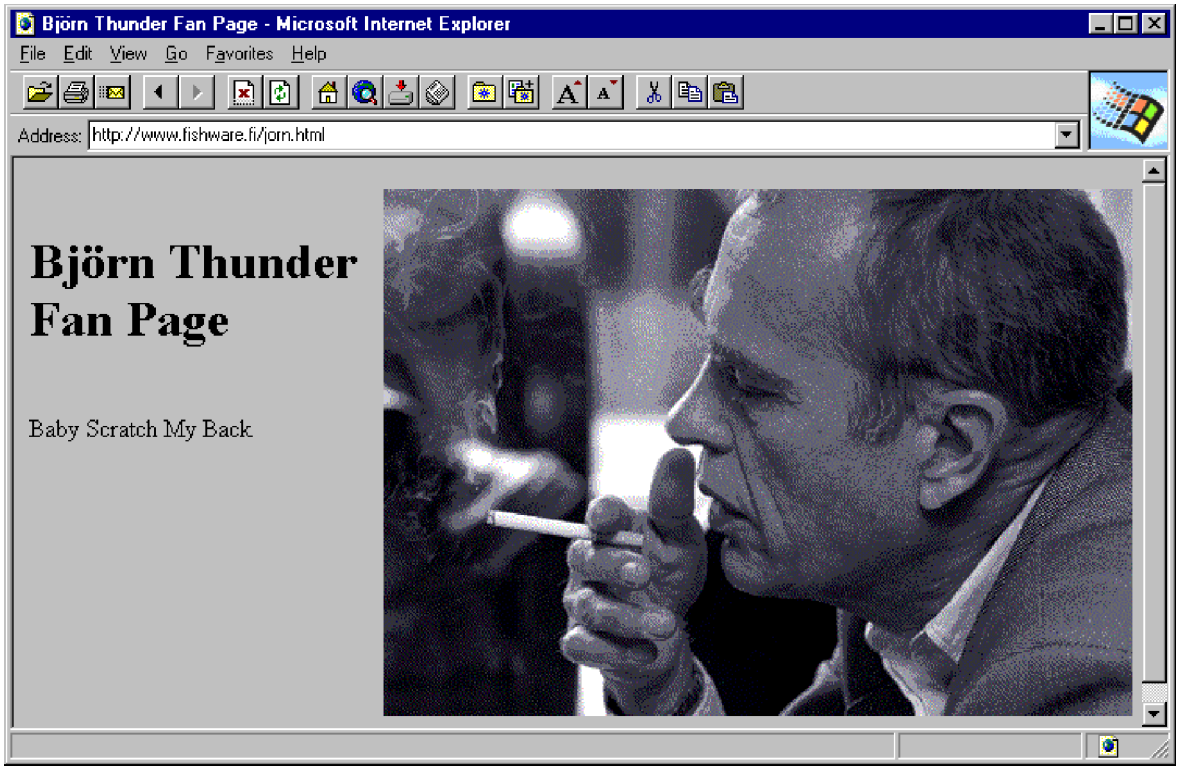
LMHOSTS-tiedoston asetukset:

```
130.10.10.5     v6    #PRE
130.9.63.5      v2    #PRE
```

Tässä esimerkissä virtuaalipalvelin on **130.10.10.5**, ja siihen voi nyt viitata osoitteilla:

- **http://130.10.10.5**
- **http://www.fishware.fi**
- **http://v6**

Tämän jälkeen hakemistoon pääsee antamalla virtuaalipalvelimen nimi:



Osoitteena voi käyttää:

- **IP-osoitetta**
- **DNS**-palvelimessa määriteltyä nimeä (esimerkiksi **www.toimialue.fi**)
- **HOSTS**-tiedostossa määriteltyä nimeä (esimerkiksi **www.toimialue.fi**)
- **NetBIOS-nimeä** (Computername, esimerkiksi **SERVERI5**)

- **LMHOSTS**-tiedostossa määriteltyä nimeä (esimerkiksi **VEPPI**)
- **WINS-palvelimessa** määritelty staattinen osoite (esimerkiksi **SERVERI5**).

Osoitteiden salliminen ja estäminen

Internet Information Serverissä on mahdollista toteuttaa **pakettien suodatus** (*Packet Filtering*) sallimalla tai kieltämällä pääsy joihinkin tiettyihin IP-osoitteisiin tietyin poikkeuksin.

Tyypillinen tilanne on se, missä halutaan sallia pääsy vain omalle aliverkolle tai aliverkolle, johon kuuluu Internet-reititin.

IP-osoitteen mukaan suodattamisen konfigurointi tapahtuu avaamalla Service Manager ja kaksoisnapauttamalla palvelinta, joka halutaan konfiguroida. Valitse **Advanced**-välilehti.

Konfigurointi tapahtuu seuraavasti:

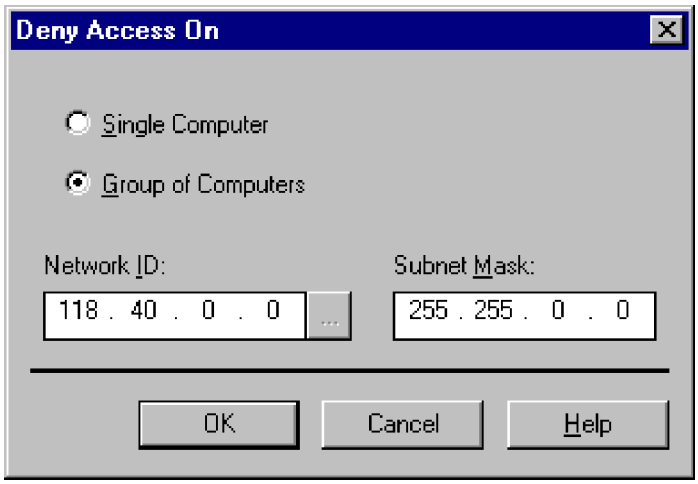
1) Valitse **Granted Access** -painike tai **Denied Access** -painike: jos valitset **Granted Access** -painikkeen, voit antaa alempaan kenttään niiden tietokoneiden IP-osoitteet, joiden pääsyä haluat **rajoittaa**. Jos valitset **Denied Access**, voit antaa kenttään niiden tietokoneiden IP-osoitteet, joille haluat sallia pääsyn IIS:ään

2) Luo poikkeukset napsauttamalla **Add**-painiketta. Esiin tulee **Grant Access On**- tai **Deny Access On** -valintaikkuna riippuen edellisestä valinnastasi

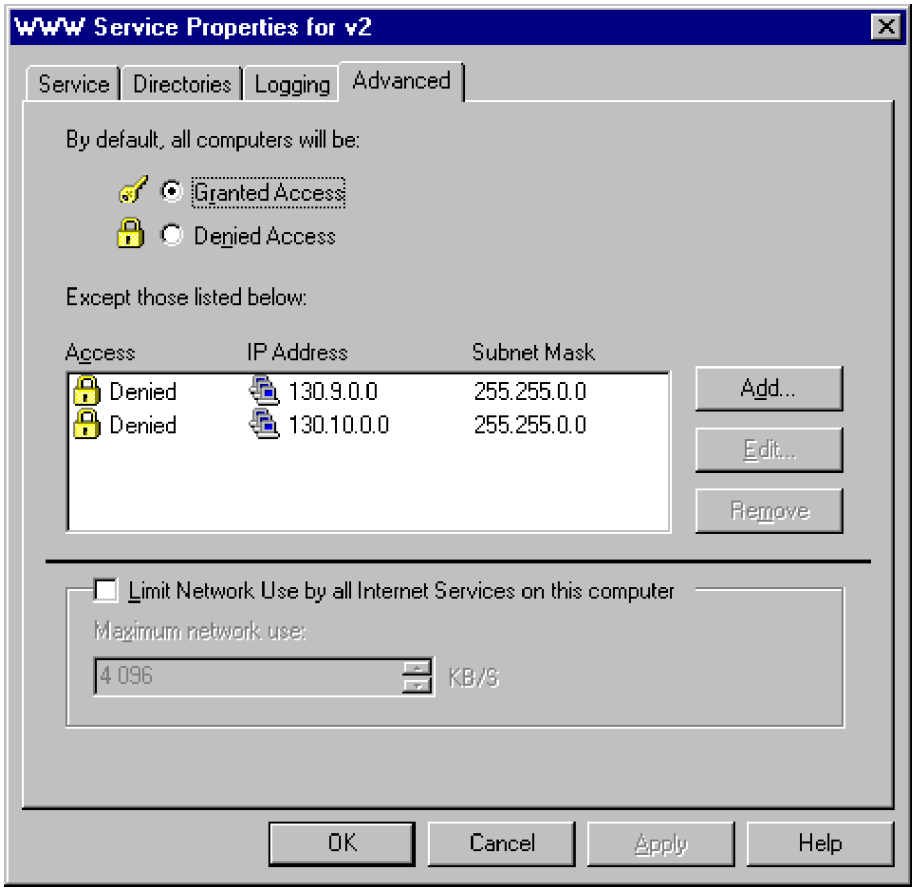
3) Tässä vaiheessa voit valita **Single Computer** ja kirjoittaa sen tietokoneen IP-osoitteen, jonka haluat sulkea pois, tai valita **Group of Computers** ja antaa IP-osoitteen ja aliverkon peitteen (*subnet mask*), jos haluat sulkea pois aliverkon:

- Jos haluat sulkea pois esimerkiksi koko luokan **C** tietokoneet, kirjoita numero muodossa **192.10.10.0**, missä **0** edustaa koko aliverkkoa

•Jos haluat sulkea pois esimerkiksi koko luokan **B** tietokoneet, kirjoita numero muodossa **120.10.0.0**, missä kaksi viimeistä nollaa edustaa koko aliverkkoa.

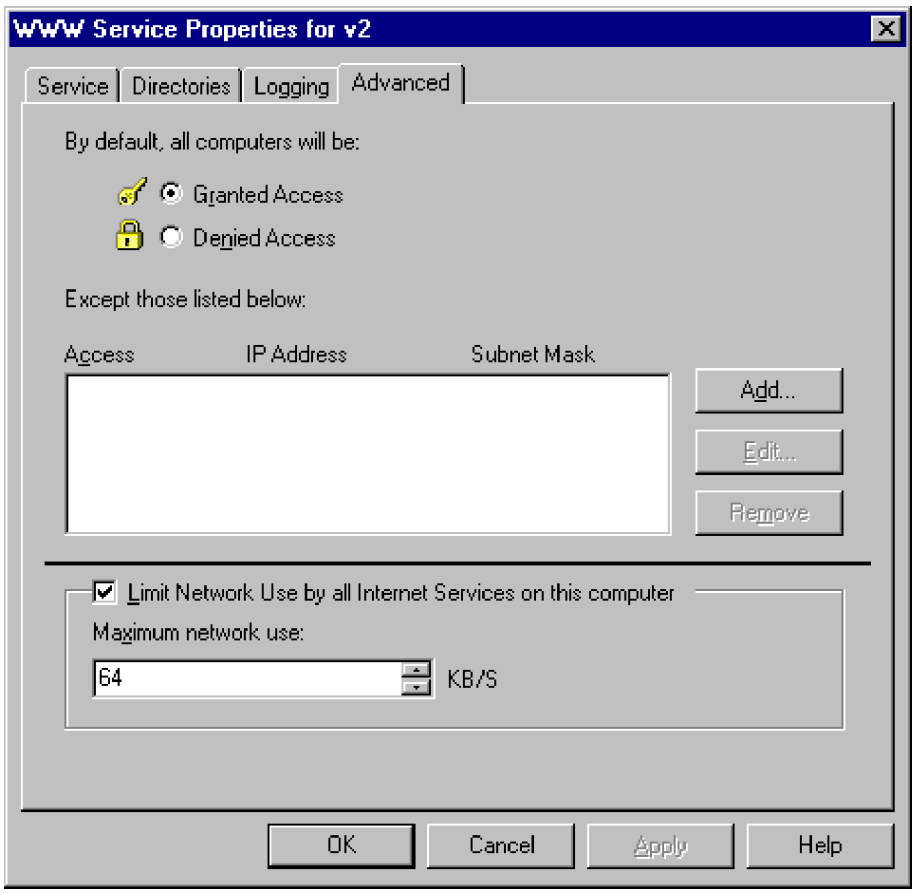


4) Paina lopuksi **OK**. Näkyviin tulee lista kielletyistä tai sallituista osoitteista.



Verkkokäytön rajoittaminen

Advanced-välilehdessä voit määritellä **Limit Network Use by all Internet Services on this computer** - kaistan rajoittaminen haluttuun määrään kilotavuja sekunnissa, kt/s (**kB/s**).

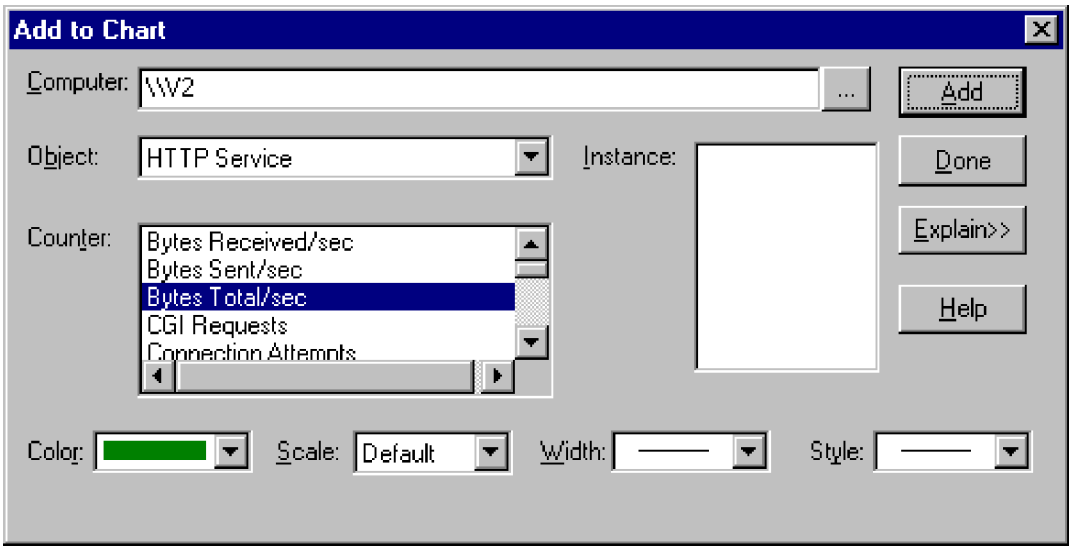


Rajoitus koskee kaikkia IIS:n palveluita, myös FTP-palvelinta.

HTTP-palvelun laskurit

Voit valvoa **Performance Monitorilla** IIS:n toimintaa.

Seuraavassa taulukossa on kuvattu objektin HTTP-palvelu (**HTTP Service**) laskurit.

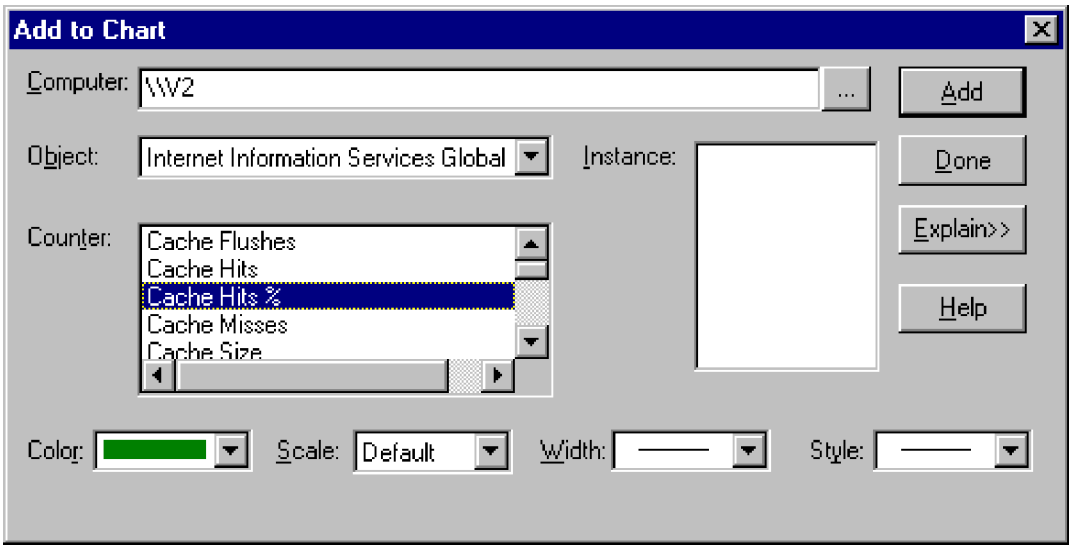


Laskuri	Kuvaus
Bytes Rec/sec	Nopeus, jolla HTTP Server vastaanottaa tavuja
Bytes Sent/sec	Nopeus, jolla HTTP Server lähettää tavuja
Bytes Total/sec	Sekunnissa lähetettyjen ja vastaanotettujen tavujen summa. Tämä on HTTP Serverin kokonaissiirtonopeus
CGI Requests	Common Gateway Interface -pyynnöt ovat räätälöityjä yhdyskäytäväsovelluksia (.EXE), joita pääkäyttäjä voi asentaa halutessaan lisätä lomakkeita ja muita dynaamisia tietolähteitä
Connection Attempts	HTTP Serveriin tehtyjen yhteysyritysten määrä
Connection/sec	Sekunnissa käsiteltävien HTTP-pyyntöjen määrä
Current Anonymous Users	Tällä hetkellä HTTP Serveriin yhteydessä olevien anonyymien käyttäjien määrä
Current CGI Requests	Tällä hetkellä HTTP Serverin yhtäaikaisesti käsittelemien CGI-pyyntöjen määrä. Tämä sisältää myös WAIS-indeksikyselyt
Current Connections	Tällä hetkellä HTTP Serveriin muodostettujen yhteyksien määrä
Current ISAPI Extension Requests	Tällä hetkellä HTTP Serverin yhtäaikaisesti käsittelemien laajennuspyyntöjen määrä
Current Noanonymous Users	Tällä hetkellä HTTP Serveriin yhteydessä olevien ei-anonyymien käyttäjien määrä
Files Received	HTTP Serverin vastaanottamien tiedostojen kokonaismäärä

Laskuri	Kuvaus
Bytes Rec/sec	Nopeus, jolla HTTP Server vastaanottaa tavuja
Files Sent	HTTP Serverin lähettämien tiedostojen kokonaismäärä
Files Total	HTTP Serverin vastaanottamien ja lähettämien tiedostojen summa. Tämä on HTTP Serverin siirtämien tiedostojen kokonaismäärä
Get Requests	GET-metodia käyttävien HTTP-pyyntöjen määrä. GET-pyyntöjä käytetään yleensä tiedostojen tai kuvakarttojen noutamiseen, vaikka niitä voidaan käyttää myös lomakkeiden kanssa
Head Requests	HEAD-metodia käyttävien HTTP-pyyntöjen määrä. HEAD-pyyntöjä käytetään yleensä, kun asiakas kyselee itsellään jo olevan asiakirjan tilaa nähdäkseen tarvitseeko se päivittää
ISAPI Extension Requests	ISAPI Extension Requests ovat räätälöityjä yhdyskäytävän dynaamisia linkkikirjastoja (.DLL), joita pääkäyttäjä voi lisätä lomakkeiden tai muiden dynaamisten tietolähteiden käsittelemiseksi
Logon Attempts	HTTP Serverin tekemien kirjautumisyritysten määrä
Maximum Anonymous Users	Samanaikaisesti HTTP Serveriin yhteydessä olevien anonyymien käyttäjien suurin mahdollinen määrä
Maximum CGI Requests	HTTP Serverin yhtäaikaisesti käsittelemien CGI-pyyntöjen suurin mahdollinen määrä. Tämä sisältää myös WAIS-indeksikyselyt
Maximum Connections	Samanaikaisesti HTTP Serveriin avoinna olevien yhteyksien suurin mahdollinen määrä
Maximum ISAPI Extension Requests	HTTP Serverin yhtäaikaisesti käsittelemien laajennuspyyntöjen suurin mahdollinen määrä
Maximum Nonanonymous Users	Samanaikaisesti HTTP Serveriin yhteydessä olevien ei-anonyymien käyttäjien suurin mahdollinen määrä
Not Found Errors	Niiden pyyntöjen määrä, joita palvelin ei voinut täyttää, koska pyydettyä asiakirjaa ei löytynyt. Yleensä tämä raportoidaan asiakkaalle HTTP 404 -virhekoodina
Other Requested Methods	Niiden HTTP-pyyntöjen määrä, jotka eivät ole GET-, POST- tai HEAD-metodeja. Metodit saattavat olla PUT, DELETE, LINK tai muita yhdyskäytäväsovellusten tukemia metodeja
Post Requests	POST-metodia käyttävien HTTP-pyyntöjen määrä. Postituspyyntöjä käytetään yleensä lomakkeissa tai yhdyskäytäväpyynnöissä

Laskuri	Kuvaus
Bytes Rec/sec	Nopeus, jolla HTTP Server vastaanottaa tavuja
Total Anonymous Users	Kaikkien joskus HTTP Serveriin yhteyden ottaneiden anonyymien käyttäjien yhteismäärä
Total Nonanonymous Users	Kaikkien joskus HTTP Serveriin yhteyden ottaneiden ei-anonyymien käyttäjien yhteismäärä

Seuraavassa taulukossa on kuvattu objektin **Internet Information Services Global** laskurit.

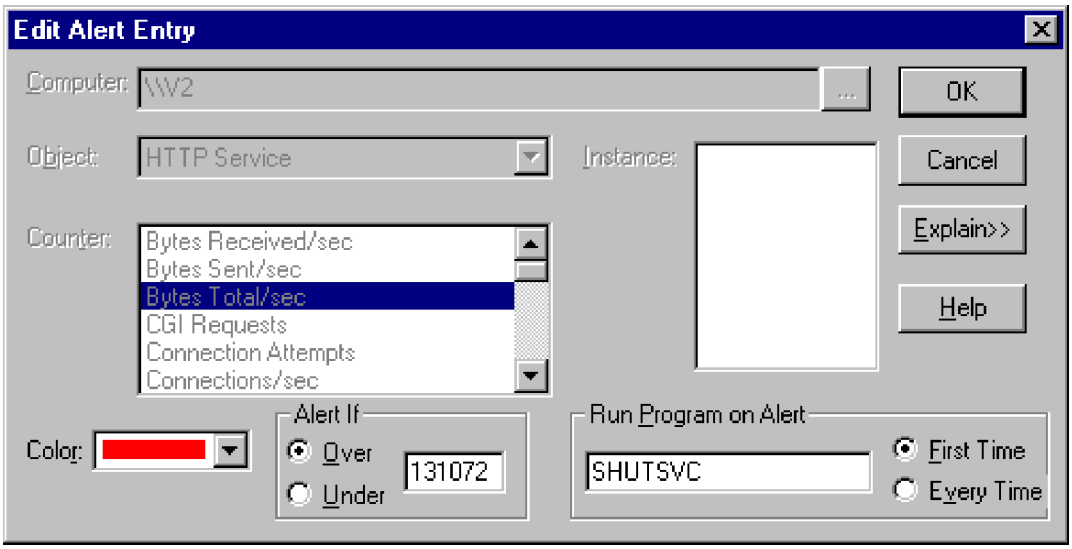


Laskuri	Kuvaus
Cache Flushes	Niiden kertojen määrä, kun välimuisti on vanhentunut Internet Information Serverin hakemistopuussa tapahtuneiden tiedosto- tai hakemistomuutoksien vuoksi
Cache Hits	Niiden kertojen kokonaismäärä, jolloin tiedoston avaus-, hakemistolistaus- tai palvelukohtainen objekti löytyi välimuistista
Cache Hits %	Niiden kertojen suhde, jolloin pyydetty tieto löytyi välimuistista, kaikkiin kertoihin, kun tietoa etsittiin välimuistista
Cache Misses	Niiden kertojen kokonaismäärä, jolloin tiedoston avaus-, hakemistolistaus- tai palvelukohtainen objekti ei löytynyt välimuistista
Cache Size	Jaetun HTTP-, FTP- ja Gopher-välimuistin suurin konfiguroitu koko
Cache Used	Jaetussa välimuistissa olevien tietoa sisältävien tavujen kokonaismäärä. Tämä sisältää hakemistolistaukset, tiedostokahvojen seurannan ja palvelukohtaiset objektit

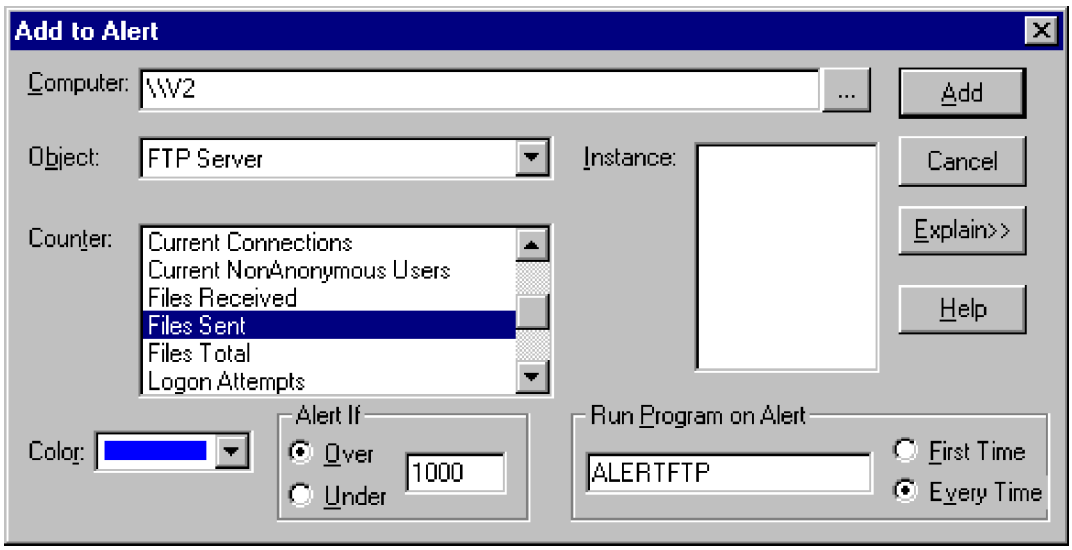
Laskuri	Kuvaus
Cache Flushes	Niiden kertojen määrä, kun välimuisti on vanhentunut Internet Information Serverin hakemistopuussa tapahtuneiden tiedosto- tai hakemistomuutoksien vuoksi
Cached File Handles	Kaikkien Internet Information Servicesien välimuistissa olevien avointen tiedostokahvojen määrä
Current Async I/O Requests Blocked	Tämänhetkiset asynkroniset I/O-pyynnöt, jotka on estetty
Directory Listings	Kaikkien Internet Information Serverin välimuistissa olevien hakemistolistausten määrä
Measured Bandwidth of Async I/O	Asynkronisen I/O:n määrä keskimäärin yhden minuutin aikana
Objects	Kaikkien Internet Information Servicesien välimuistissa olevien objektien määrä. Tämä sisältää hakemistolistaukset, tiedostokahvojen seurannan ja palvelukohtaiset objektit
Total Async I/O Requests Allowed	Sallittujen asynkronisten I/O-pyyntöjen kokonaismäärä
Total Async I/O Requests Blocked	Estettyjen asynkronisten I/O-pyyntöjen kokonaismäärä
Total Async I/O Requests Rejected	Hylättyjen asynkronisten I/O-pyyntöjen kokonaismäärä

Suorituskyvyn seurannan lisäksi voit luoda hälytyksiä (Alerts), jos IIS on kovin kuormitettu.

Tässä esimerkissä valvotaan **HTTP Servicen** kuormitusta; jos **Bytes Total/sec** on yli **128 kt/s**, ajetaan palvelu alas komentojonolla **SHUTSVC**.



Tässä tapauksessa halutaan ylipäätään halytys, kun FTP-palvelimelta on imuroitu 1000 tiedostoa. Komentorivin komento on **ALERTFTP**.



Internet Information Serverin optimointi

Seuraavaksi muutamia tapoja tehostaa Internet Information Serverin toimintaa:

- Lisää keskusmuistia (64 Mt käyttökelpoinen, 128 Mt ruuhkaisilla palvelimilla)
- Siirrä muut palvelut toisiin palvelimiin
- Käytä IIS-palvelimena **Stand-alone Server**-tyyppistä palvelinta
- Käytä DNS:n *Round-robin* -menetelmää: jos käytössäsi on useampia IIS-palvelimia, voit määritellä saman IIS-palvelimen nimen osoittamaan eri IP-osoitteisiin. Tällöin DNS ohjaa aina seuraavan pyynnön seuraavalle osoitteelle eli voit tasata kuormitusta eri palvelimien välillä
- Käytä tiedostojen sirpalointiin sopivaa apuohjelmaa, esimerkiksi **Diskeeper** (**http://www.execsoft.com**) tai **SpeedDisk** (**http://www.symantec.com**).

Secure Sockets Layer

Secure Sockets Layer on tietoturvaprotokolla, joka toimii TCP/IP-yhteyksien ja HTTP-palvelun välissä. Sitä voidaan käyttää **Internet Explorer** WWW-asiakassovellusten ja **Internet Information Serverin** kanssa.

Siinä on seuraavat ominaisuudet:

- Tiedon salaus tiedonsiirron turvaamiseksi
- Palvelimen tunnistus luotettaviin kirjautumisiin
- Viestin eheyden tarkistus, jotta voidaan varmistua, että viestiä ei ole peukaloitu.

Lisätietoja löytyy osoitteesta **http://www.rsa.com**.

Istunnon alussa tapahtuu asiakkaan ja palvelimen välillä kättely (*Handshaking*), jossa asiakas ja palvelin sopivat yhteyden varmistamisessa käytettävästä turvatasosta. Varmistuksen jälkeen käynnistyy normaali HTTP-yhteysistunto, paitsi että kaikki asiakkaan ja palvelimen välillä kulkeva tieto salataan. Salattavaa tietoa on mm.:

- Asiakkaan pyytämä URL
- Käyttäjän lomakkeille syöttämä tieto, kuten esim. luottokorttien numerot
- Kirjautumistiedot, kuten käyttäjätunnukset ja salasanat
- Kaikki palvelimen asiakkaalle lähettämät tiedot.

SSL vaatii koko joukon toimenpiteitä asetusten määrittelemiseksi ja aktivoimiseksi, mutta kun se on kerran saatu toimimaan, vain SSL:ää tukevat asiakkaat voivat käyttää sillä suojattuja hakemistoja. Yksi vaadittava toimenpide on ottaa yhteyttä sertifiointilaitokseen, jotta saisit tietoturvajärjestelmällesi sertifikaatin (et siis voi odottaa tekeväsi näitä toimia muutamassa minuutissa).

Seuraavassa on luettelo tärkeimmistä asioista, jotka pitää ottaa huomioon SSL:n käyttöönotossa:

- Luo avainpari ja pyyntötiedosto. Avainparissa on julkinen ja salainen avain
- Ota yhteys serfikaatteja myöntävään laitokseen ja pyydä tietoturva-avaimillesi sertifikaatti
- Asenna sertifiointilaitokselta saamasi sertifikaatti palvelimellesi
- Käynnistä Internet Service Manager ja aktivoi SSL-käyttäjätunnistus
- Aktivoi SSL niissä hakemistoissa, jotka vaativat suojausta, tai aktivoi se WWW-kotihakemistosi juurihakemistossa (joka on yleensä \WWWRoot).

Asiakasohjelmat voivat kommunikoida WWW-palvelimen SSL-suojattujen hakemistojen kanssa ainoastaan käyttämällä URL-osoitteissaan alkutun-

nistetta **https**, eikä **http**.

Erota suojatut hakemistot julkisista hakemistoista, äläkä tee alihakemistoja hakemistoihin, joita **ei** ole suojattu SSL:llä.

Avainparin luominen

Ensimmäinen vaihe on luoda avainpari. Siihen on kaksi mahdollisuutta:

- **Key Manager**-ohjelma
- **KEYGEN**-ohjelma, joka löytyy hakemistosta, jonne olet asentanut Internet Information Serverin:
  - **KEYPAIR.KEY** - avaintiedosto, joka sisältää avainparin
  - **REQUEST.REQ** - sertifikaatin pyyntötiedosto.

Palvelimellesi on luotava ns. **Fully Distinguished Name** (Ominaisnimi) käyttämällä seuraavia muuttujia:

C = Kaksikirjaiminen maanimen ISO-koodi (esim. US, FR, FI, AU, UK, DE)

S = Osavaltio tai lääni (esim. Washington, Alberta tai California).
Älä lyhennä tätä nimeä

L = Paikkakunta (esim. Redmond, Kouvola tai Turku)

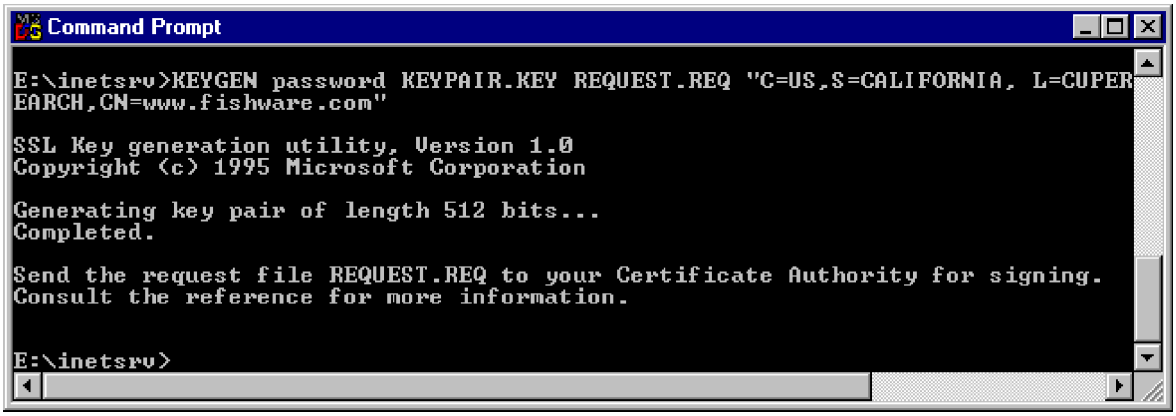
O = Organisaatio (Mielellään ISO-rekisteröity, ylätason organisaatio tai yrityksen nimi)

OU = Organisaatioyksikkö (kuten esim. osaston nimi)

CN = Common Name (Palvelimen toimialueen nimi, esim. www.fishware.com)

Esimerkiksi Kaliforniassa Cupertinossa sijaitsevan Fishware-yrityksen tuotekehitysosaston ominaisnimi olisi:

C=US,S=CALIFORNIA,L=CUPERTINO,O=FISHWARE,OU=RESEARCH,CN=www.fishware.com



Älä käytä missään kentässä pilkkuja, koska ne tulkitaan kentän loppumerkiksi.

Alla on esimerkki KEYGEN:in käytöstä **KEYPAIR.KEY**- ja sertifikaatin pyyntötiedoston **REQUEST.REQ** tekemiseksi käyttäen yllä kuvattua ominaisnimeä. Korvaa sana *password* sopivalla salasanalla.

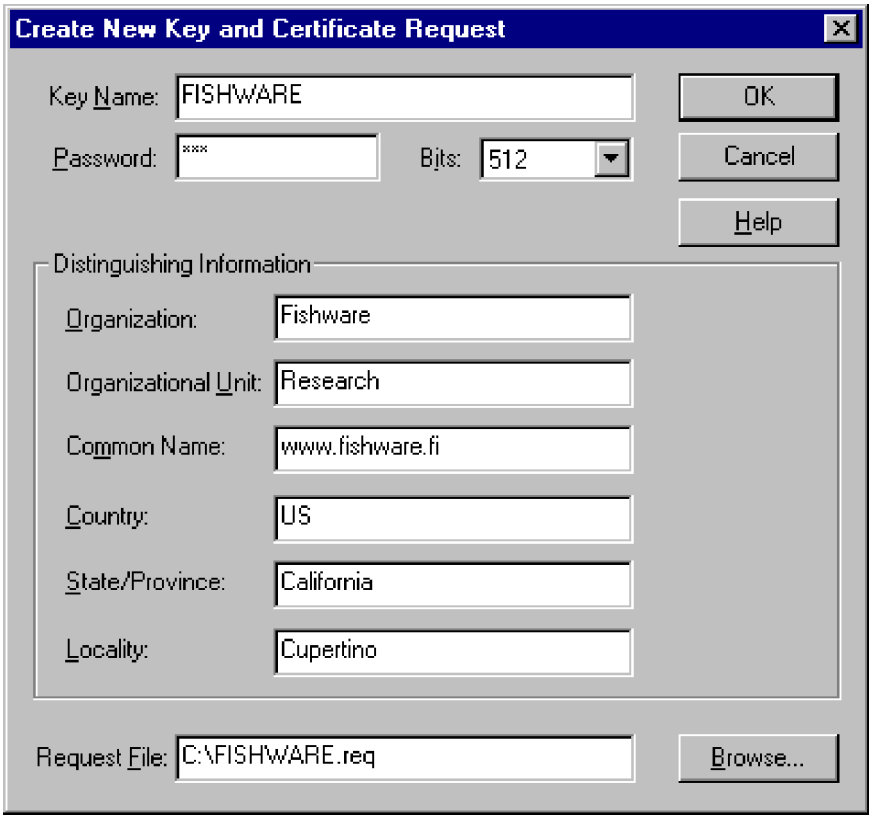
KEYGEN password KEYPAIR.KEY REQUEST.REQ
C=US,S=CALIFORNIA,
L=CUPERTINO,O=FISHWARE,OU=RESEARCH,CN=www.fishware.com

Tämä kehittää seuraavan viestin ja tallentaa tiedostot nykyiseen hakemistoon:

Jos suoritat KEYGEN.EXEn useammin kuin kerran, saat virheilmoituksen 80, joka osoittaa, että tiedosto on jo olemassa.

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBOjCB5QIBADCBgDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCllvdXIgU3RhdGUMBAGA1UECxMJWW91ciBVbml0MRkwFwYDVQQDFBBZb3VylE5ldCBBZGRyZXNzMKoZIhvcNAQEEBQADQQA8t8EQO7WfmlerP7ca57Xf+27/81+tnOu2NviVDhQq
KoZIhvcNAQEEBQADQQA8t8EQO7WfmlerP7ca57Xf+27/81+tnOu2NviVDhQqbbNg
-----END NEW CERTIFICATE REQUEST-----

Saman voit tehdä myös käyttöliittymän kautta **Key Manager**-ohjelmalla.



Huomaa, että voit antaa sertifikaatin pyyntötiedoston nimen Request File-kohtaan.

Webmaster: xyz@xyz.com
Phone:
Server: Microsoft Key Manager for IIS 2.0
Common-name: jne
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBOjCB5QIBADCBgDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCllvdXIgU
3RhdGUMBAGA1UECxMJWW91ciBVbml0MRkwFwYDVQQDFBBZb3VyIE5ld
CBBZGRyZXNzMKoZIhvcNAQEEBQADQQA8t8EQO7WfmlerP7ca57Xf+27/81+
tnOu2NviVDhQq
KoZIhvcNAQEEBQADQQA8t8EQO7WfmlerP7ca57Xf+27/81+tnOu2NviVDhQq
bbNg
-----END NEW CERTIFICATE REQUEST-----

Sertifikaatin pyytäminen

Kun olet luonut pyyntötiedoston, sinun täytyy pyytää sertifiointilaitosta sertifioimaan se. Microsoft suosittelee käyttämään VeriSign-laitosta osoitteessa **http://www.verisign.com**, vaikka voit toki käyttää muitakin. Näin sertifiointi tapahtuu VeriSign-laitoksen kanssa:

1) Kirjoita kirje, josta selviää organisaatiosi verkon pääkäyttäjä, ja josta ilmenee organisaatiosi virallinen nimi

2) Faksaa tämä kirje Verisignille yrityksesi kirjepaperilla ja varmista, että pyydät **Digital ID**:tä **Microsoftin Internet Information Serverille**. VeriSign antaa jatko-ohjeet. Voit myös käydä vilkaisemassa heidän kotisivujaan osoitteessa **http://www.verisign.com** ja saada lisätietoja.

Palvelimen sertifiointi

Sen jälkeen, kun olet pyytänyt sertifikaattia sertifiointilaitokselta, saat allekirjoitetun sertifikaatin. Se on tekstitiedosto, jossa on pitkä jono koodattuja kirjaimia. Kopioi tiedot tekstitiedostoon käyttämällä mitä tahansa tekstieditoria. Anna tiedostolle nimeksi vaikkapa **SSLCODE.-TXT**.

Anna seuraavanlainen **SETKEY**-komento (olettaen, että annoit tiedostolle nimeksi SSLCODE.TXT). Sijoita sanan *password* paikalle sopiva salasana ja **ip_address**-sanan tilalle sen palvelimen IP-osoite, jonka haluat sertifioida. Jos et määrittele IP-osoitetta, samaa sertifikaattia käytetään kaikkien järjestelmän virtuaalipalvelinten sertifiointiin.

```
SETKEY password KEYPAIR.KEY SSLCODE.TXT ip_address
```

Tallenna **KEYPAIR.KEY**-tiedosto levykkeelle ja poista se kiintolevyltä. Tallenna levyke varmaan ja turvalliseen paikkaan. Varmista myös, ettet unohda salasanaa. **SETKEY.EXE**:n ajamisen jälkeen käynnistä WWW-palvelu uudelleen, jolloin SSL otetaan käyttöön.

Saman voit tehdä myös käyttöliittymän kautta **Key Manager**-ohjelmalla.

SSL:n aktivointi

SSL otetaan käyttöön WWW-palvelimessa käynnistämällä Internet Service Manager ja kaksoisnapauttamalla haluttua palvelinta. Näin otat käyttöön käyttäjätunnistuksen ja tietoturvaominaisuudet:

1) Ota HTTP-käyttäjätunnistus käyttöön valitsemalla **Service**-välilehdessä **Windows NT Challenge/Response**

2) Kaksoisnapauta **Directory Properties** -valintaikkunassa hakemistoa, joka tarvitsee suojattuja yhteyksiä. Valitse **Directory Properties** -valintaikkunassa **Require Secure SSL Channel** -valintaa

3) Jos hakemisto ei ole vielä listassa, valitse **Add**-painike, ja lisää hakemisto täyttämällä valintaikkunan kentät. Voit käyttää SSL:n tietoturvaominaisuuksia missä tahansa WWW-palvelimen virtuaalihakemistossa.

Microsoft Index Server

Microsoft Index Server on ilmainen indeksointiohjelmisto Internet Information Serveriin. Microsoft Index Serverillä on kaksi päätehtävää:

- **Indeksointi** - Index Server etsii julkaistuja dokumentteja, käy läpi niiden sisällön (jos kyseessä on HTML-, Word- tai Excel-dokumentti), kerää tiedot muista ominaisuuksista (tiedostonimi, tekijä, hakusanat) ja varastoi kaikki nämä tiedot indeksiin

- **Kyselyt** - Index Server toteuttaa käyttäjien hakuja ja luo linkkilistan löytyneistä dokumenteista.

Index Server käyttää hyväkseen useita muitakin komponentteja, ja saatat joutua muuttamaan niiden asetuksia Index Serverin käyttöönoton yhteydessä.

Index Server on helppo asentaa ja ylläpitää. Sen indeksointi- ja hakutoiminnot ovat tehokkaita, mutta jos haluat indeksoida **etäkoneiden** doku-

mentteja, joudut luultavasti asentamaan muitakin työkaluja.

Index Serverin voi imuroida Microsoftin WWW-palvelimelta, **http://www.microsoft.com**.

Käyttöönotto

Näin otat Index Serverin käyttöön:

1) Asenna **Internet Information Server**

2) Konfiguroi IIS:n paikalliset- ja virtuaalihakemistot

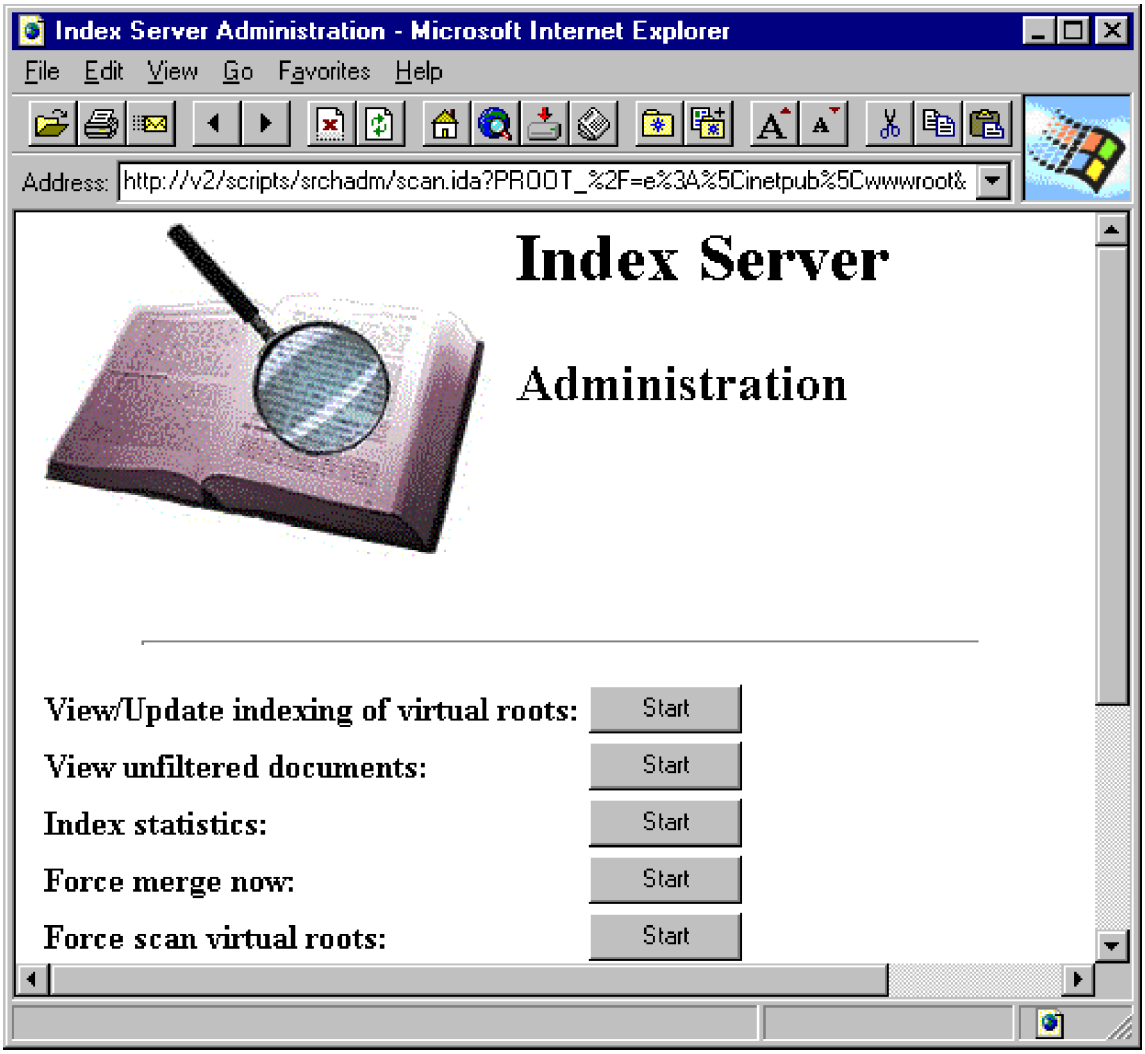
3) Muokkaa jokaisen virtuaalihakemiston asetuksia niin, että IIS:n käyttäjätunnuksella on oikeus lukea kaikkia indeksoitavia tiedostoja. Paikallisten virtuaalihakemistojen osalta tulee varmistaa, että järjestelmän käyttäjätunnuksella (**System**) on pääsy kaikkiin indeksoitaviin tiedostoihin

4) Asenna **Index Server**. Asennus tapahtuu tyypillisesti ajamalla jokin exe-tiedosto paikallisesti palvelimella. Asennus ei edellytä palvelimen uudelleenkäynnistystä

5) Asennuksen jälkeen testaa Index Serverin toiminta ja luo HTML-lomake, jonka avulla käyttäjät voivat tehdä hakuja. Voit muokata valmista mallisivua **samples/search/queryhit.htm**.

Index Server Administration

Asennuksen jälkeen käynnistysvalikon Programs-valikosta löytyy **Microsoft Index Server**-valikko. Yksi sen valinnoista on Index Serverin selainpohjainen hallintaohjelma **Index Server Administration**.



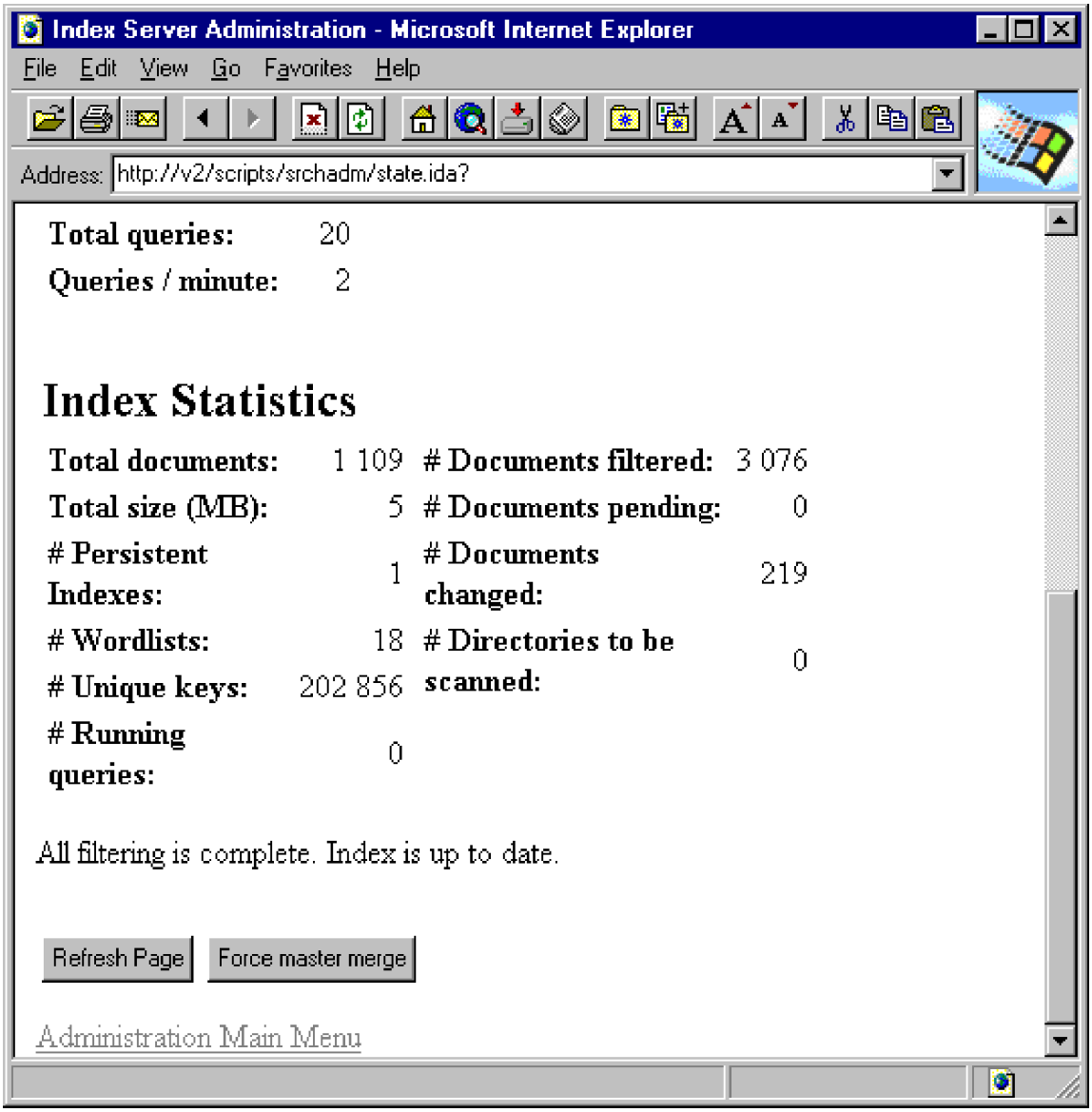
Valinnat ovat seuraavat:

- **View/Update indexing of virtual roots** - voit valita indeksoitavat hakemistot
- **View unfiltered documents** - voit tarkistaa käsittelemättömät tiedostot
- **Index statistics** - tilastotiedot indeksoinnista

- **Force merge now** - lisätään uusien tiedostojen indeksit
- **Force scan virtual roots** - suoritetaan kaikkien virtuaalihakemistojen indeksointi.

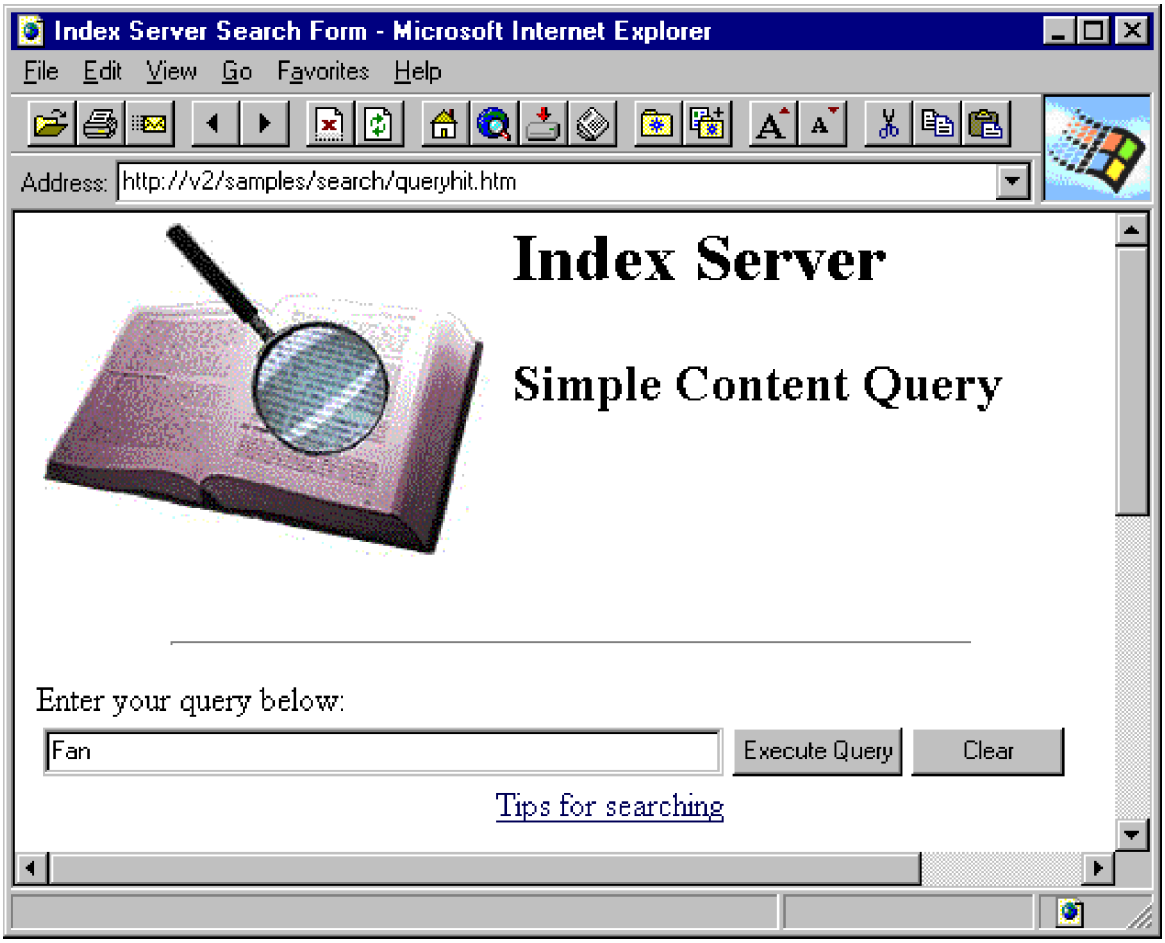
Kysely

Tarkista ennen kyselyä, että indeksi on ajantasalla **Index Server Administration** -ohjelman **Index statistics** -valinnalla.



Esimerkkikyselypohja on **samples/search/queryhit.htm**.

Valitsemalla **Index Server Sample Query Form** voit tehdä kyselyitä. Painamalla **Tips for searching** saat lisäohjeita - yksinkertaisin kysely on yksi sana:



Painamalla **Execute Query** kysely ohjataan Index Serverille, joka palauttaa vastaussivun:

Haussa voit käyttää myös valmiita malleja esimerkiksi hakuun tiedostokoon perusteella.

Haussa voit käyttää loogisia operaattoreita:

- *-merkki kosvaa loput merkit
- ** -kaikki sanan muodot
- **NEAR** ja **AND** - Bill NEAR Redmond
- **AND NOT** - CD-ROM AND NOT Audio
- **OR** - Wolf OR Blonde

Indeksointi

Index Server aloittaa virtuaalijuurten indeksoinnin ensimmäisellä kerralla, kun kysely tehdään. Tämän jälkeen palvelin päivittää indeksit aina automaattisesti. Kun palvelin vastaanottaa kyselyn, se tarkistaa indeksin, etsii dokumentit jotka täsmäävät kyselyyn ja luo löytyneistä dokumenteista HTML-linkkilistan käyttäjälle.

Indeksoitavat hakemistot määritellään IIS:ssä, ja niiden käyttöoikeudet ovat Windows NT:n käyttöoikeusjärjestelmän mukaiset.

Paikallisten hakemistojen indeksointi

Paikallisten hakemistojen indeksointi käy seuraavasti:

1) Käynnistä **Internet Service Manager**

2) Valitse **Directories**-välilehti ja napauta **Add**-painiketta lisätäksesi fyysistä hakemistoa vastaavan virtuaalihakemiston. **Index Server** indeksoi kaikki virtuaalihakemistoissa olevat tiedostot.

Etähakemistojen indeksointi

Etähakemistojen indeksoinnissa tarvittavat toimet riippuvat siitä, viittaako IIS hakemistoon UNC-nimellä vai levyaseman kirjaimella. IIS viittaa Microsoft-palvelinten (Windows NT ja Windows 95) hakemistoihin UNC-nimellä ja NetWare-palvelinten hakemistoihin levyasematunnuksella.

Jotta voitaisiin indeksoida NetWare-palvelimen tietoja, on otettava käyttöön **Gateway Services for NetWare**. Tämä tehdään Ohjauspaneelissa valitsemalla **Network**-kuvakkeen **Services**-välilehti, napauttamalla **Add**-painiketta ja valitsemalla palvelu **Gateway (and Client) Services for NetWare**.

Hakemistoihin viittaaminen UNC-nimillä

IIS käyttää jaettuja hakemistoja aina jonkin käyttäjätunnuksen avulla. Kun määrittelet käyttäjätunnuksen, sen oikeuksiksi riittää pelkkä lukuoikeus: jos et määrittele mitään oikeuksia, Index Server ei pääse käsiksi tiedostoihin, ja jos määrittelet täydet oikeudet, jokaisella tavallisellakin käyttäjällä on rajoittamaton pääsy tiedostoihin.

Kun määrittelet UNC-polkua virtuaalihakemistoon, muista määritellä käyttäjätunnuksen yhteydessä myös toimialueen tai palvelimen nimi, esimerkiksi **FISHWARE\IndexUser**, ei pelkkä **IndexUser**. Muista käyttää kenoviivaa kauttaviivan sijaan, **ei FISHWARE/IndexUser**. IIS sallii kirjoittaa tiedot kummalla tahansa tavalla ja korjaa nämä virheet automaattisesti, mutta Index Server **ei**. Jaetun hakemiston sisältö näkyy IIS:ssä, mutta Index Server ei pysty indeksoimaan sitä.

Hakemistoihin viittaaminen levyasematunnuksella

IIS ja Index Server käyttävät NetWare-hakemistoyhteyksiin aina sen ylläpitäjän käyttäjätunnusta, joka on määritellyt verkkoyhteyden **Gateway Services for NetWare**:n avulla. Koska tämä tunnus on jo valmiiksi olemassa, ei sitä tarvitse luoda, ja koska yhteyskin on jo olemassa, ei virtuaalihakemistoa luotaessa tarvitse antaa käyttäjätunnusta eikä salasanaa. Muodosta yhteys jaettuun hakemistoon yhdistämällä jokin levyasematunnus verkkoasemaan **Windows NT Explorerissa** tai käytä **NET USE** -komentoa komentoriviltä.

Luo virtuaalihakemisto Internet Service Managerilla: avaa **WWW**-palvelun ominaisuudet, valitse **Directories**-välilehti ja määrittele virtuaalihakemiston tiedot.

Virtuaalipalvelinten hakemistojen indeksointi

Yhdellä IIS-palvelimella voi olla useita virtuaalipalvelimia. Toisinaan käyttäjän haku saattaa käsittää useita virtuaalipalvelimia. Index Server ylläpitää erillisiä indeksejä eri virtuaalipalvelimille, joten yhdeltä virtuaalipalvelimelta lähetetty haku ei tutki toisen virtuaalipalvelimen indeksiä. Jos yhteishaku useilta virtuaalipalvelimilta on tarpeen, luo hakemistorakenne sellaiseksi, että kaikki etsittävät hakemistot ovat yhden hakemiston alihakemistoja. Kohdista sitten haku yhteiseen päähakemistoon.

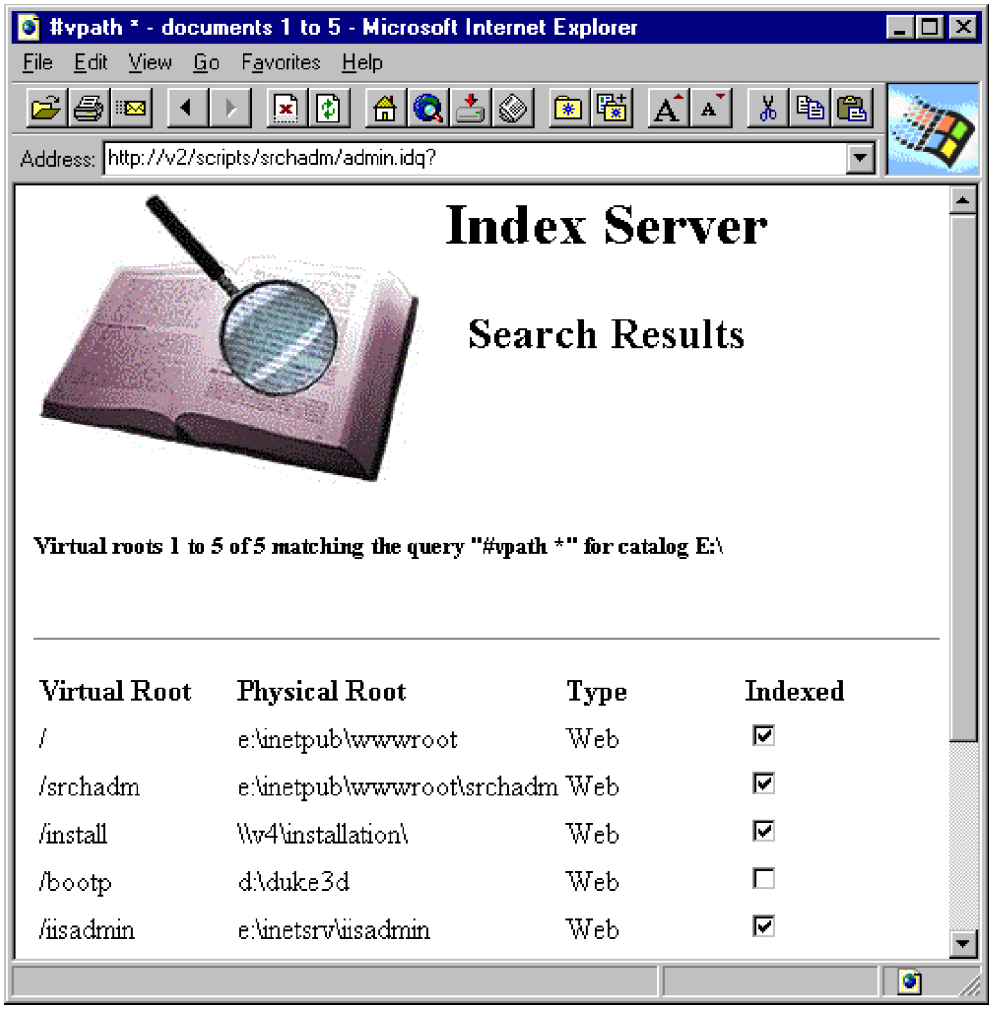
Huomaa, että kullakin WWW-palvelimella jokin virtuaalipalvelimista on **oletuspalvelin**. Jos indeksoit muun kuin oletuspalvelimen, Index Server indeksoi yleensä **myös** oletuspalvelimen.

Indeksoinnin estäminen

Osa materiaalista voi olla sellaista, jota et halua indeksoida. Tällaisia ovat esimerkiksi luottamukselliset, puutteelliset tai vanhentuneet tiedot.

Yksinkertaisimmillaan voit estää koko virtuaalijuuren indeksoinnin. Jos virtuaalijuuri **/FW** vastaa hakemistoa **D:\FFEEDER\FW** eikä yksikään virtuaalijuuri osoita hakemistoon **D:\FFEEDER**, voit estää indeksoinnin Index Serverin Administration-välilehdeltä.

Käynnistä **View/Update indexing of virtual roots**, valitse virtuaalijuuri **/FW** ja poista valinta ruudusta **Indexed**.



Jos haluat estää vain joidenkin tiedostojen indeksoinnin, käytettävissä on erilaisia keinoja riippuen tiedostomuodosta ja siitä, onko tiedosto paikallisella tai verkon NTFS-levyllä vai FAT-levyllä.

HTML-tiedostot

HTML-tiedoston indeksoinnin voit estää lisäämällä metakomennon:
<meta name= robots content= noindex >

Windows-verkon etätiedostot

Jos tiedosto on virtuaalijuuressa, joka sijaitsee jaetulla Windows NT:n tai Windows 95:n hakemistossa, yksinkertaisinta on poistaa lukuoikeus Index Serverin käyttämältä käyttäjätunnukselta. Jos samalla palvelimella on dokumentteja useissa alihakemistoissa, voit poistaa käyttöoikeudet siltä hakemistolta, jossa luottamukset tiedot ovat.

Paikalliset NTFS-hakemistot

Estääksesi paikallisella NTFS-levyllä olevien virtuaalijuurten käytön poista sen tunnuksen käyttöoikeudet, jonka alaisuudessa käyttäjän selain muodostaa yhteyden. Jos anonyymiyhteydet on sallittu, tämä tunnus on käytetty anonyymitunnus, muussa tapauksessa käyttäjän oma tunnus.

Toinen vaihtoehto on asettaa yksittäisten .HTM-, .HTX-, .IDQ-, ja .HTW-tiedostojen oikeudet.

Paikalliset FAT-hakemistot

Jos hakemisto on paikallisella FAT-levyllä, edellä mainittuja turvakeinoja ei voi käyttää. FAT ei salli tiedostojen suojaamista käyttäjätunnuksen perusteella.

Yksi mahdollisuus on muuttaa kyselylomakkeen HTML-koodia niin, että Index Server ei palauta kaikkia kyselyn tuloksena löytyneitä tiedostoja, vaikka ne sisältyvätkin indeksiin.

Microsoft Proxy Server

Microsoft Proxy Server tarjoaa mahdollisuuden valvoa sitä, miten yksittäiset käyttäjät pääsevät internetiin esimerkiksi FTP-tai Gopher-protokollalla tai WWW-palvelujen kautta.

Proxy Server antaa sisäisille käyttäjille mahdollisuuden käyttää oman verkon ulkopuolella olevia resursseja ja estää ulkopuolisten yritykset käyttää sisäistä verkkoa. Ulkoinen verkko on tavallisesti internet, mutta se voi olla myös joku muu *epäluotettava* verkko.

Proxy Server toimii siten, että kun sisäisen verkon (*intranetin*) käyttäjä yrittää ottaa yhteyden internet-osoitteeseen, Proxy Server sieppaa viestin, paketoi sen uudelleen ja lähettää pyynnön edelleen kohdepalvelimelle. Kun internet-palvelin vastaa, Proxy Server vastaanottaa vastauksen, varmistaa, että vastaus on autenttinen ja lähettää sen edelleen sisäiselle asiakkaalle.

Tämä on kaikkien välitys- eli proxy-palvelimien käyttämä menetelmä, jolla piilotetaan sisäiset verkko-osoitteet. Internetistä ei päästetä sisäiseen verkkoon paketteja, joita joku ei ole sisäisestä verkosta pyytänyt. Sisäiset järjestelmät voidaan turvata ja itse proxy-palvelimesta tulee keskitetysti hallittu järjestelmä, jossa voidaan noudattaa tiettyjä turvakäytäntöjä. Proxy-palvelin on oikeastaan turvayhdyskäytävä, joka liittää toisiinsa kaksi erilaista verkkoa ja samalla valvoo sekä ohjaa niiden välistä liikennettä. Tämän tarkoituksena on suojella sisäisiä resursseja luvattomalta käytöltä.

Tämän lisäksi Proxy Server tarjoaa välimuistin (*Cache*), joka nopeuttaa internet-hakuja sekä vähentää internet-liikennettä.

Ominaisuudet

Kun sisäisen verkon asiakasohjelma haluaa tehdä pyynnön internet-palvelimelle, Proxy Server hoitaa pyynnön edelleen. Asiakasselaimet ohjaavat Winsock-pyyntönsä Proxy Serverille käytössä olevan protokollan avulla. Proxy Server välittää pyynnöt internetiin käyttämällä Winsockia TCP/IP:n kautta. Proxy Server tukee useimpia internet-protokollia, muun muassa HTTP:tä ja FTP:tä sekä RealAudiota, VDOLiveä, IRC:tä sekä posti- ja uutisprotokollia.

Sisäisissä verkoissa voidaan käyttää myös Novellin IPX/SPX-protokollaa, jolloin organisaation ei tarvitse siirtyä TCP/IP-protokollan käyttöön. IPX/SPX-liikenne voidaan reitittää sekä internet-palvelimelle että sisäisille intranet-palvelimille.

Proxy Server on yhteensopiva CERN:in proxy-protokollan kanssa, josta on käytännössä tullut proxy-palvelujen standardi. Palvelin hyväksyy proxy-pyynnöt selaimilta, jotka ovat yhteensopivia CERN:in proxy-protokollan kanssa, esimerkiksi **Internet Explorer** ja **Netscape Navigator**.

Proxy Serverin ominaisuuksia:

- Proxy-palvelu ja protokollamuunnin tarjoavat yhteyden liittää muita kuin TCP/IP-verkkoja (esimerkiksi IPX-verkkoja) muihin verkkoihin. Proxy Server ja Windows Socket Service tuovat internet-sovellukset käyttöön standardiprotokollien välityksellä. Kun käyttäjä tekee pyynnön internetiin WWW-, Gopher- tai FTP-palvelulla, Proxy Server muodostaa palvelimen puolesta TCP/IP-yhteyden osoitteeseen. Se hyväksyy vastaukseksi internetistä ainoastaan ne vastaukset, jotka tulevat siitä osoitteesta, johon pyyntö lähetettiin. Jos sisäinen käyttäjä ei ole pyytänyt pakettia, sitä ei oteta vastaan

- Salaus mahdollistaa turvatun tiedonsiirron internetin kautta salausprotokollien avulla esimerkiksi **Secure Sockets Layer** (SSL) ja **Private Communication Technology** (PCT)

- Palomuuriominaisuudet (*Firewall*) sisältävät mahdollisuuksia muodostaa turvallinen palomuuri estämään ja suodattamaan verkkoliikennettä

- Pääkäyttäjät voivat myöntää tai kieltää käyttäjän, palvelun, portin tai IP-osoitteen pääsyn resurssiin. Pääsy tiettyihin osoitteisiin voidaan estää

- Suodattamalla toimialueiden nimiä voidaan valvoa, mitä internet-resursseja sisäisen verkon käyttäjät saavat käyttää. Sallituista ja kielletyistä internet-toimialueista (*internet domain*) tehdään luettelo, jonka perusteella luodaan säännöstö. Kun se otetaan käyttöön, se vaikuttaa kaikkiin käyttäjiin, jotka ottavat yhteyden internetiin Proxy Serverin kautta. Käyttäjille ja käyttäjäryhmille voidaan määrittää oikeuksia WWW:n, Gopherin ja FTP:n käyttöön. Käyttäjätason valvonta taas on integroitu

Windows NT:n toimialue- ja käyttäjätunnusominaisuuksiin, ja verkon pääkäyttäjät voivat näin valvoa, kenellä on oikeus käyttää internetiä.

- Proxy-palvelin suodattaa ja monistaa WWW-sivujen sisältöä ja myös tallettaa **välimuistiin** usein käytettyjä WWW-sivuja ja -dokumentteja. Suosituimmat WWW-sivut päivitetään automaattisesti. Välimuistin käyttö säästää kaistanleveyttä, koska WWW-sivut voidaan hakea suoraan välimuistista kaikille niitä tarvitseville sisäisille käyttäjille. Välimuistin käyttö voi laskea käyttäjän pyynnön toteuttamiseen tarvittavan ajan lähes puoleen

- Pääkäyttäjät voivat valvoa välimuistissa olevia tietoja ja määrittää, kuinka paljon levytilaa välimuistille ja sen sisältämille tiedoille annetaan sekä määrittää **Time out**- ja **Refresh**-ajat. Välimuistin käyttö on erityisen kätevää pienissä yrityksissä, joiden yhteys internetiin on hidas ja joiden asiakasohjelmat käyttävät samoja internet-resursseja.

Toimintaperiaate

Kaikki yhteydet palvelimen ja asiakkaan välillä tapahtuvat HTTP-protokollan välityksellä. HTTP on pyyntö- ja vastauskomentoprotokolla, jota asiakkaat ja palvelimet käyttävät tietojen kyselyyn, pyyntöjen täyttämiseen, vastausten hyväksymiseen ja kuittaamiseen.

Kun proxy-palvelin sijaitsee asiakas- ja kohdepalvelimen välissä HTTP pyyntö- ja vastauskäytäntö muuttuu hieman:

1) WWW-asiakasohjelma tekee tietylle internetin WWW-palvelimelle pyynnön kuten tavallista

2) Proxy Server tarkistaa asiakkaan ja kohteen välisen tilan. WWW-palvelin vastaanottaa pyynnön ja tarkistaa, onko asiakasohjelmalla lupa käyttää tällaista yhteyttä

3) Proxy Server tarkistaa, saako käyttäjä tehdä pyyntöjä kyseiselle toimialueelle (*internet domain*)

4) Proxy Server tarkistaa välimuistista (*Cache*), onko pyydetty dokumentti välimuistissa. Jos dokumentti on välimuistissa, proxy-

palvelin palauttaa sen asiakkaalle

5) Jos pyydetty dokumentti ei ole välimuistissa, Proxy Server pyytää sitä määritetyltä WWW-palvelimelta

6) Kohdepalvelin palauttaa dokumentin Proxy Serverille

7) Proxy Server palauttaa dokumentin asiakasohjelmalle.

Ennen asennusta

Proxy Server toimii Windows NT -palvelimessa, johon on asennettu kaksi verkkokorttia. Näiden korttien välinen reititys täytyy estää, jotta toisen verkon liikenne ei pääse toiseen verkkoon. Internet-yhteydestä täytyy myös estää palvelut ja tietyt liitännät. Proxy Server hoitaa tästä eteenpäin kaiken liikenteen näiden kahden verkon välillä:

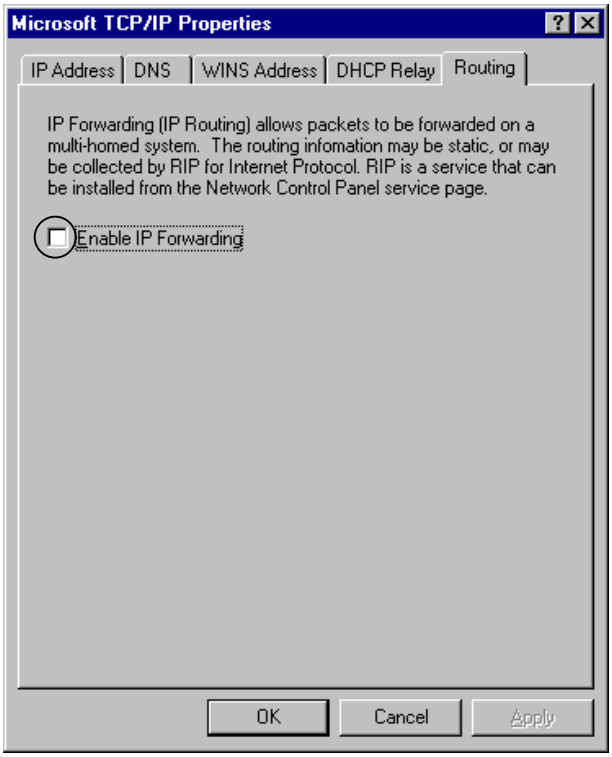
- Lähiverkkoon liitetty verkkokortti käyttää RPC-proseduurikutsuja internet-kyselyjen ja vastausten välittämiseen verkossa
- Lähiverkko voi käyttää TCP/IP:tä, IPX/SPX:ää, NetBEUI:a ja muita protokollia
- Internetiin liitetyn verkkokortin täytyy käyttää TCP/IP-protokollaa
- Proxy Server valvoo yhteyksiä ja kääntää protokollia sisäisen ja ulkoisen verkon välillä.

Jos haluat käyttää **vain** Proxy Serverin **välimuistiominaisuuksia**, yksikin verkkokortti riittää. Tämä on hyvä vaihtoehto turvatuissa sisäisissä verkoissa, joissa suojaukset on hoidettu muilla menetelmillä, esimerkiksi erillisillä palomuureilla (*Firewall*).

Proxy Serverin asentamiseen tarvitaan Windows NT Server 4.0. Microsoft suosittelee, että palvelin asennetaan NT-toimialueelle **Stand-alone Serveriksi** (ei siis ohjauskoneeksi), vaikka sekin on mahdollista. Jos halutaan käyttää suojausominaisuuksia, palvelimeen täytyy asentaa **kaksi verkkokorttia**.

Varmista, että TCP/IP-protokolla on asennettu oikein Ohjauspaneelin **Network**-toiminnolla. TCP/IP liitetään internetiin liitettyyn verkkokorttiin. Älä käytä tässä verkkokortissa muita protokollia, kuten IPX/SPX:ää tai NetBEUI:a. Sisäisen verkon liitäntään voidaan kuitenkin sitoa (*bind*) joko TCP/IP tai IPX/SPX.

Kun protokollat on asennettu, reititys verkkokorttien välillä täytyy estää poistamalla **Routing**-välilehden **Enable IP Forwarding**-asetus. Tämä on erityisen tärkeää, jos sekä sisäinen että ulkoinen verkko käyttävät TCP/IP-protokollaa. Estoa tarvitaan kieltämään liikenne ulkoisen ja sisäisen verkon välillä.



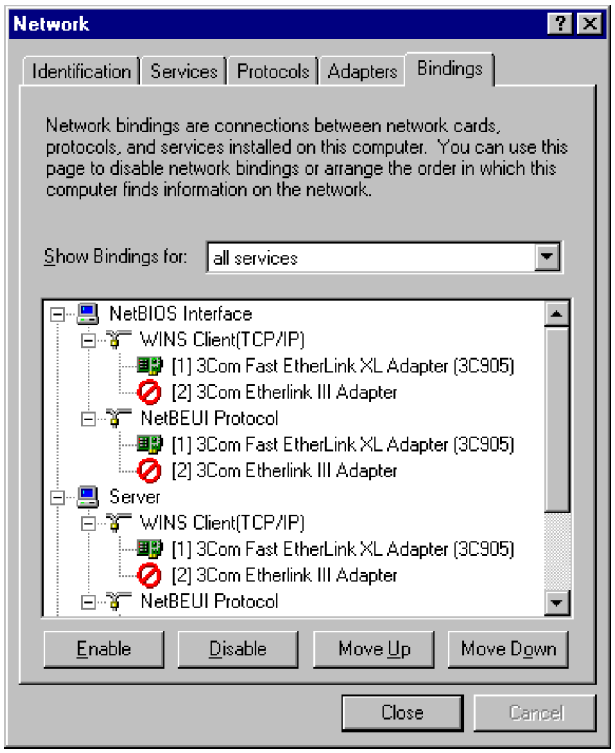
Jos reititys on käytössä, sisäiseen verkkoon on suora pääsy. Asetus on rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\TcpIp\Parameters**
Nimi	**IPEnableRouter**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei käytössä (oletus) - 1 käytössä**

Tämä avain määrittää, onko reititin käytössä vai ei. Jos tunkeutuja pääsee käsiksi tähän asetukseen, hän voi avata reitityksen. Vain **Administrators**-ryhmällä ja **System**-käyttäjätunnuksilla tulisi antaa oikeudet muuttaa tätä arvoa.

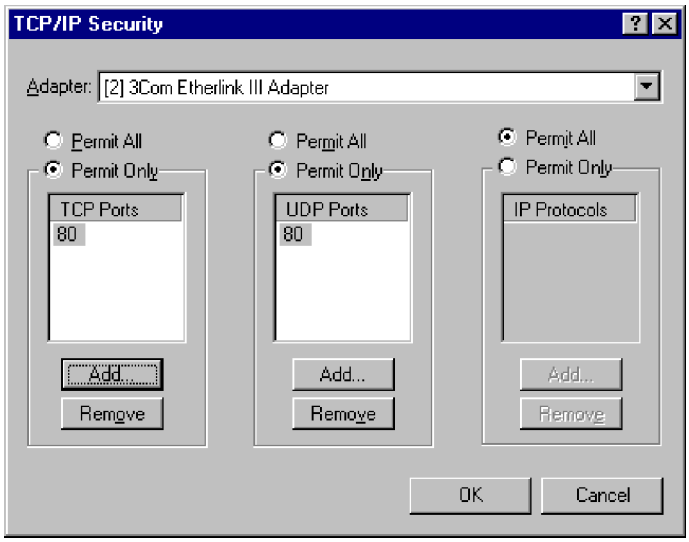
Lisää varotoimia:

- Käytä vain NTFS-tiedostojärjestelmää
- Estä **User Manager for Domain**issa oikeus, joka sallii pääkäyttäjien kirjautumisen palvelimelle verkon kautta (**Access this computer from network**). Näin tunkeutujia estetään hyökkäämästä verkkoon pääkäyttäjien tunnusten kautta
- Sulje tarpeettomat palvelut Ohjauspaneelin **Services**-toiminnolla
- Varmista, että **Guest**-tunnuksen käyttö on estetty (**Disabled**) ja että **Everyone**-ryhmällä on hakemistoissa vain lukuoikeudet
- Jotta vain määrätyt käyttäjät voisivat käyttää Proxy Serveriä, poista **Everyone**-ryhmältä **Access this computer from network**-oikeus ja luo sitten uusi yleinen ryhmä (esim. **Internet-users**) ja anna sille **Access this computer from network**-oikeus
- Tarkista **Administrators**-ryhmän jäsenet ja poista asiaankuulumattomat jäsenet. Proxy Server voidaan perustaa omaksi toimialueekseen, josta sitten luodaan luottosuhde toiseen toimialueeseen. Luotettu toimialue sisältää niiden käyttäjien käyttäjätunnukset, joilla on lupa käyttää palvelinta ja näin voidaan rajoittaa Proxy Serverin käyttöä käyttäjätunnusten avulla
- Tarkista **User Manager for Domain**issa, että valvonta (**Audit**) on käytössä
- Poista SMB-palvelujen (palvelin (**Server**), työasema (**Workstation**) ja **NetBIOS**) sidos internetiin liitettyyn verkkokorttiin (kuvassa **3Com EtherLink III**)



- Koska Proxy Serveriä ei suositella tiedostopalvelimeksi, kannattaa ehkä katkaista sidokset näihin palveluihin myös sisäisestä verkosta. Sisäiset ja ulkoiset käyttäjät voivat yhä käyttää Proxy Serverin HTTP-palveluja, jos se määritetään palvelimella.

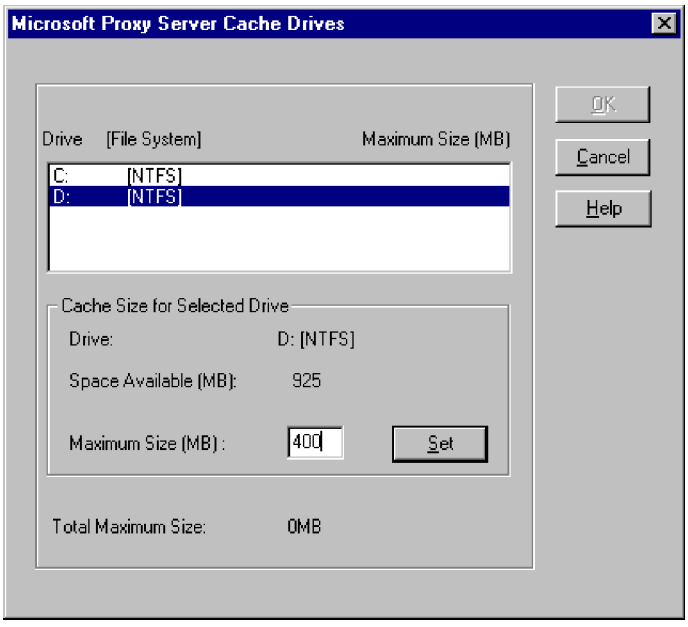
- Myös internetiin liitetyn rajapinnan porttien käyttö täytyy estää. Paina **TCP/IP Address**-välilehden **Advanced**-painiketta, valitse **Enable Security** ja napauta **Configure**-painiketta. Valitse **Adapter**-listasta internetiin kytketty verkkokortti ja paina **Add**-painiketta lisätäksesi haluamasi palvelun porttinumero. Portin numero on **80** (HTTP-palvelu), mutta voit lisätä myös muita portteja. Kun olet määrittänyt portit, palvelin täytyy käynnistää uudelleen.



Asentaminen

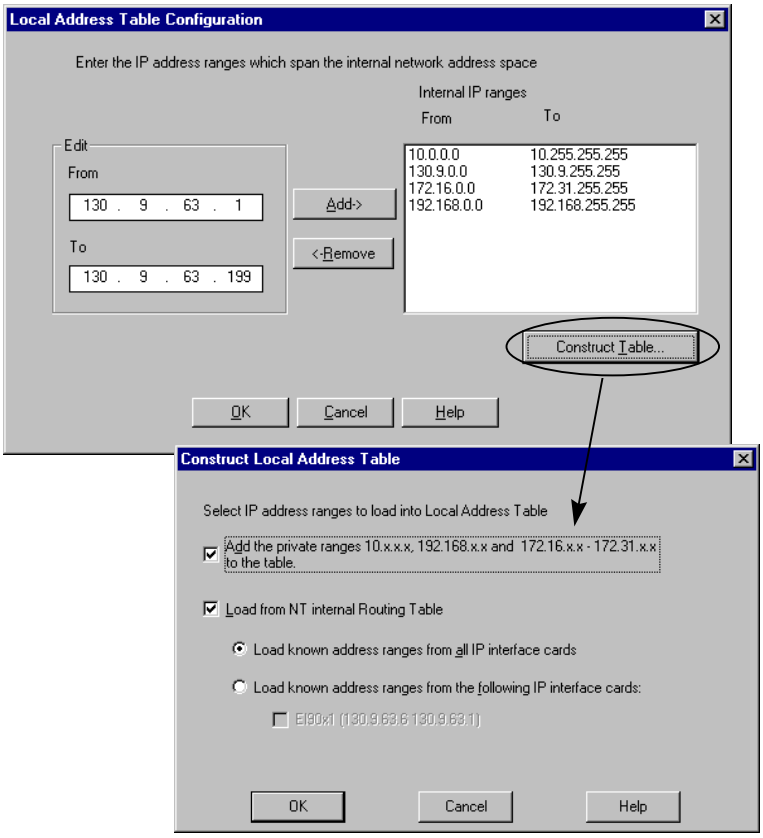
Kun edelliset toimet on tehty, voit kirjautua pääkäyttäjätason tunnuksella ja ajaa Proxy Serverin asennusohjelman (**SETUP.EXE**).

Valitse hakemisto, johon haluat asentaa Proxy Server -ohjelman ja vastaa kysymyksiin, mitkä komponentit haluat asentaa, mitä asiakastyyppejä haluat tukea ja missä välimuistin levyasemat (**Server Cache Drives**) sijaitsevat. Väimuisti voi sijaita useammassakin levyasemassa.



Sinulta pyydetään myös niiden *sisäisten* verkkojen IP-osoitteita, joilla on oikeus käyttää Proxy Serveriä. Proxy Server määrittää niiden avulla, millä asiakasohjelmilla on oikeus käyttää ulkoista verkkoa ja yrittääkö asiakas päästä jonnekin, mihin sillä ei ole lupaa ottaa yhteyttä. IP-osoitteet syötetään pareina, jotka määrittävät IP-osoitealueen, jokaisen asiakkaan IP-osoitetta ei siis tarvitse syöttää erikseen. Osoitepareja säilytetään **Local Address Tablessa** (LAT), joka on Proxy Serverin **CLIENT** -hakemistossa sijaitseva **MSPLAT.TXT**-tekstitiedosto.

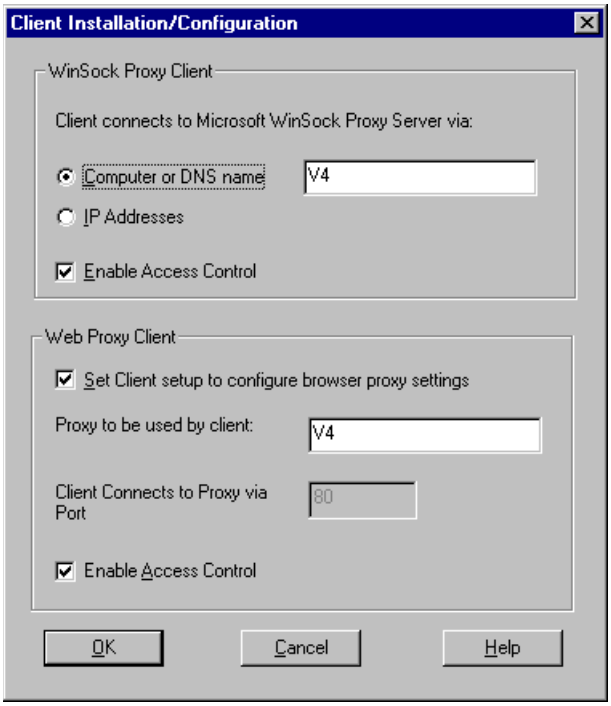
Painikkeella **Contruct Table** voit lisätä LAT:iin tyypilliset sisäiset osoitesarjat sekä reititystaulun.



LAT poimitaan asiakasohjelmille, jotka on määritetty käyttämään palvelua. Etä-Winsock-asiakas, joka haluaa päästä johonkin IP-osoitteeseen, voi etsiä taulukosta tietoa, kuuluuko pyydetty osoite sisäiseen vai ulkoiseen verkkoon. Jos osoite on ulkoisessa verkossa, pyyntö lähetetään käsiteltäväksi Proxy Serverille. Huomaa, että jos asiakasohjelma yrittää päästä internetiin Proxy Serverin kautta ja asiakas ei ole rekisteröity osoite, pääsy kielletään.

LAT:iin ei pitäisi tallentaa mitään ulkoisia (internet-) IP-osoitteita. Proxy Server nimittäin pitäisi näitä osoitteita sisäisinä ja siitä seuraisi turvallisuusongelmia, koska määritetyillä tietokoneilla ajettavat asiakasohjelmat pääsisivät sisäiseen verkkoon.

Kun IP-osoitteet on määritetty, voidaan määrittää Proxy Serverin asiakasasetukset. Esille tulee **Client Installation/Configration** -ikkuna, jossa voidaan määrittää, kuinka asiakkaiden asennusohjelmat konfiguroivat asiakkaiden yhteyksiä Proxy Serveriin (asennuksen apuna voi käyttää **System Management Server**iä). Myös käytönvalvonta (**Enable Access Control**) voidaan valita, jolloin esimerkiksi joko kaikki sisäiset asiakkaat voivat käyttää Windows Socket -palvelua, tai määrittää, että vain **Internet Service Managerissa** erikseen määritetyt asiakkaat voivat käyttää sitä.



Kun nämä asetukset on tehty, Proxy Server-palvelimen asennusohjelma suoritetaan loppuun ja muut asetukset voidaan määrittää **Internet Service Manager**issa.

Web Proxy Servicen konfigurointi

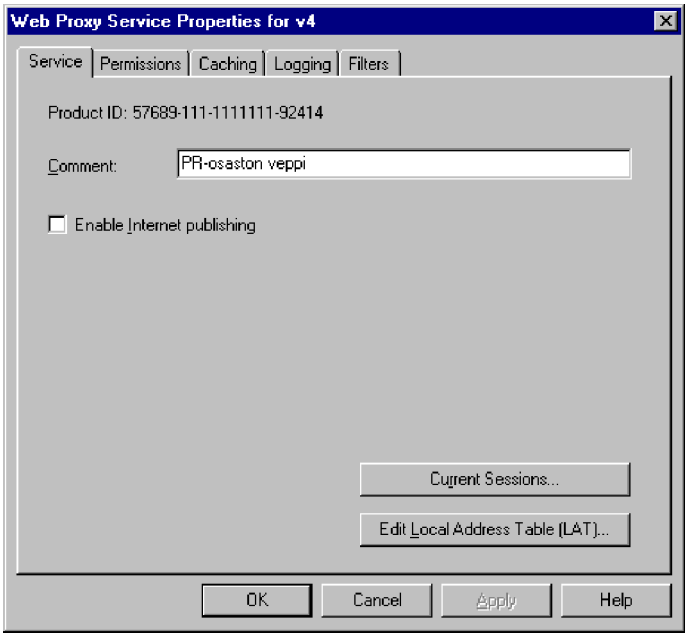
Proxy Serveriä voidaan konfiguroida **Internet Service Manager**illa. Esimerkin tapauksessa Windows NT 4.0:n IIS:n tarjoamat FTP-, Gopher- ja WWW-palvelut on asennettu palvelimelle ja nekin näkyvät ikkunassa. Haluttua palvelua voidaan ohjata kaksoisnapauttamalla sitä. Silloin esille tulee ominaisuusikkuna, jossa voidaan määrittää palvelun ominaisuuksia.

Voit määritellä sekä **Web Proxy Servicen** että **WinSock Proxy**-palvelun asetuksia. **WinSock Proxy**-palvelun asetuksia on käsitelty myöhemmin.

Välilehdet ovat seuraavat:

- **Service** - palvelun yleiset asetukset
- **Permissions** - salli tai kiellä palvelun käyttö
- **Caching** - välimuistin asetukset
- **Logging** - lokitiedoston asetukset
- **Filters** - salli tai kiellä pääsy tiettyihin IP-osoitteisiin.

Service

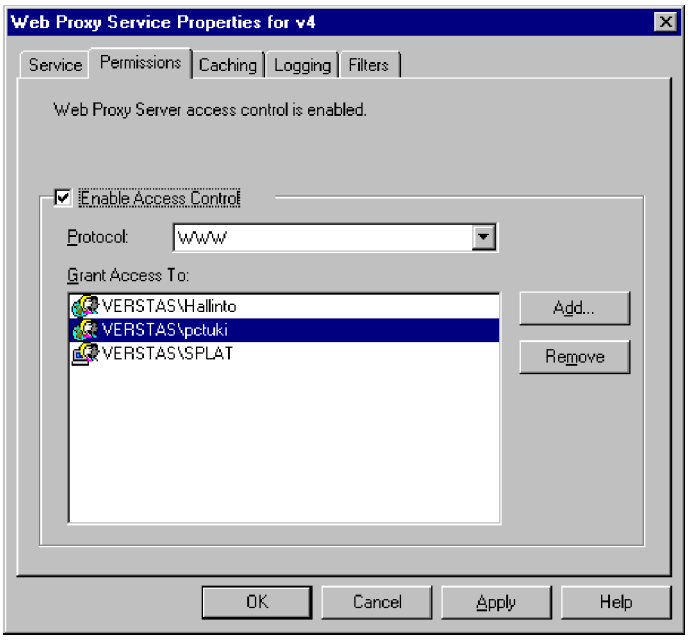


Asetukset ovat seuraavat:

- **Comment** - voit kirjoittaa kommentin palvelusta
- **Enable Internet publishing** - jos Proxy Serverissä on asennettuna myös IIS, määritellään, onko IIS sallittu myös internetin kautta - oletuksena **ei** ole. Valitse rasti, jos on tarkoitus, että esimerkiksi WWW-palvelimeen pääsee internetistä
- **Current Session** -painikkeella pääset katsomaan luetteloa käyttäjistä, jotka ovat lähettäneet proxy-palvelimelle pyyntöjä
- **Edit Local Address Table** - voit muokata LAT:ia.

Permissions

Permissions-ikkunassa voidaan määrittää käyttäjän oikeudet eri protokollille. Asetukset ovat protokollakohtaiset!



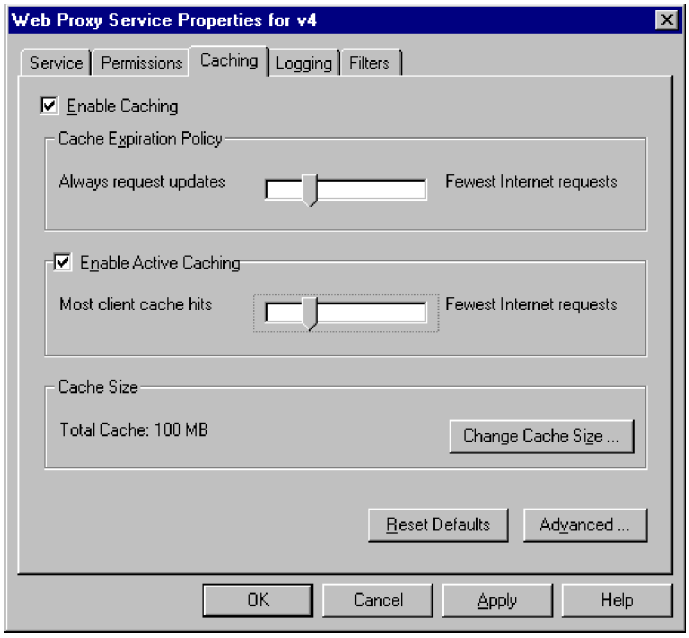
Asetukset ovat seuraavat:

- **Protocol** - FTP Read (FTP-palvelimen lukuoikeus), Gopher, WWW tai Secure (Secure Sockets Layer)

- **Grant Access To** - valitse käyttäjiä ja ryhmiä, joille annetaan oikeus käyttää kyseistä palvelua internetissä. Kun Add-painiketta napsautetaan, esille tulee käyttäjätunnuslista, josta voidaan valita nykyiseltä tai joltain muulta toimialueelta käyttäjiä ja ryhmiä, joille myönnetään oikeus käyttää palvelua.

Caching

Caching-välilehdessä asetetaan Proxy Serverin välimuistin käyttö ja asetukset ovat seuraavat:



- **Enable Caching** - onko välimuisti käytössä - jos ruutu on valittu, määritä sitten seuraavasti muut vaihtoehdot. Levyn välimuisti tallentaa kopion jokaisesta verkon asiakkaiden käyttämästä kohteesta. Jos joku toinen tarvitsee samaa kohdetta, se noudetaan välimuistista, ellei se ole vielä vanhentunut. Proxy Server voi tarvita suurenkin välimuistin riippuen käyttäjien käyttötottumuksista ja käytön määrästä

- **Cache Expiration Policy** - määrittää välimuistin sisältämien kohteiden tuoreuden eli sen, kuinka kauan kohteen välimuistissa olevaa paikallista kohdetta käytetään ennen kuin internetistä noudetaan uusi kappale. Valitse sopiva aika vetämällä valitsinta. Sopiva aika löytyy lähinnä kokeilemalla

- **Active Caching Policy** - kuinka usein välimuistin kohteita **päivitetään automaattisesti**. Jos valitsin on lähempänä vaihtoehtoa **Most client cache hits**, välimuistia päivitetään usein. Jos se on lähempänä vaihtoehtoa **Fewest Internet requests**, välimuistia päivitetään harvemmin

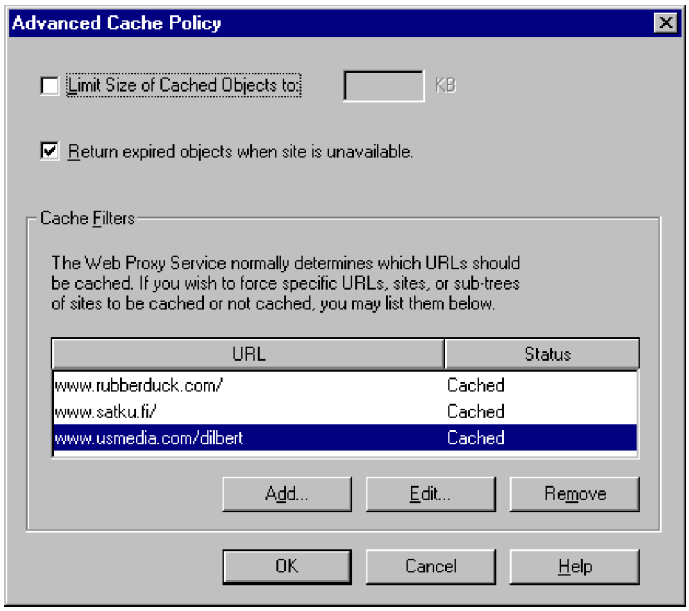
- **Cache Size** - määrittää välimuistin koon.

- **Advanced**-painikkeella päästään **Advanced Cache Policy**-ikkunaan:

  - **Limit Size of Cached Objects to** - välimuistin tallentamien kohteiden maksimikoko

  - **Return expired objects when site is unavailable** - jos kohteeseen ei saada yhteyttä ja jos välimuistissa olevat tiedot **eivät** ole vanhentuneet, tiedot palautetaan asiakkaalle välimuistista

  - **Add**-painikkeella voit lisätä ja **Edit**-painikkeella voit muokata kohteet, jotka tallennetaan aina tai ei koskaan välimuistiin.

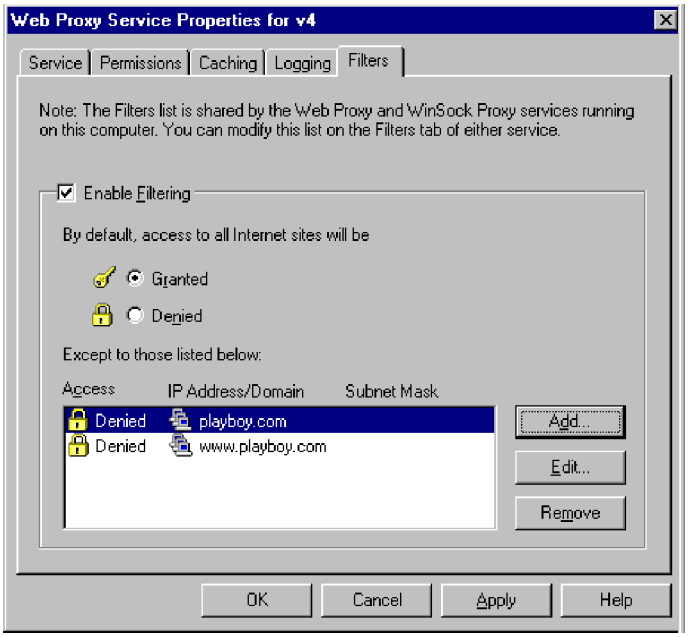


Logging

Lokit toimivat kuten Internet Information Serverin lokit, ks. asetukset IIS:n kohdalta aiemmin tässä luvussa.

Filters

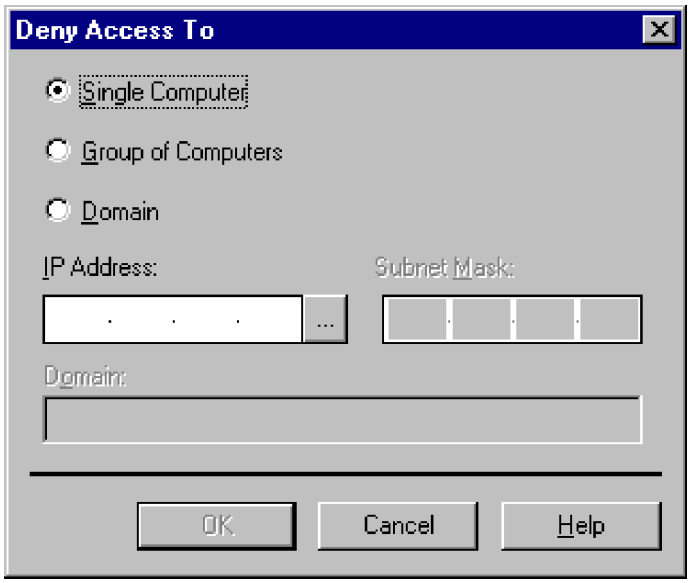
Proxy Serverin suodatus asetetaan Filters-välilehdessä:



Ikkunassa voidaan ottaa suodatus käyttöön (**Enable Filtering**) ja määrittää, millaista suodatusta halutaan käyttää. Voidaan joko myöntää (**Granted**) pääsy kaikkiin internet-osoitteisiin tai kieltää pääsy (**Denied**) kaikkiin internet-osoitteisiin ja luetella sitten poikkeukset.

Jos esimerkiksi sallitaan (**Granted**) pääsy kaikkiin internet-osoitteisiin, voidaan kirjoittaa poikkeusluetteloon (**Except...**) ne sivut tai IP-osoitteet, joihin pääsyä ei haluta sallia. Poikkeusluetteloon voidaan määrittää yksittäinen IP-osoite tai IP-osoitealue (esimerkiksi tietyn organisaation kaikki palvelimeet) tai toimialueiden nimiä.

Poikkeukset luodaan napauttamalla **Lisää**-painiketta: valitse joko **Single Computer**, **Group of Computers** tai **Domain** ja täytä sitten **IP Address**-kenttä tai **Domain**-kenttä. Huomaa, että toimialueen nimi voi olla yksittäisen tietokoneen nimi tai toimialueen nimi, joka tarkoittaa useita tietokoneita.



WinSock Proxy Servicen konfigurointi

Windows Sockets on sovellusohjelman rajapinta (API), jonka avulla ohjelmoijat rakentavat toistensa kanssa verkon yli kommunikoivia sovelluksia. Tarkemmin sanoen Sockets on prosessien välinen kommunikointimenetelmä, jonka avulla palvelimet ja niiden asiakkaat muodostavat yhteyden tiedonsiirtoa varten. Kaikki yhteyden muodostamiseen, tiedon lähettämiseen ja vastaanottamiseen sekä yhteyden sulkemiseen liittyvät parametrit määritetään Windows Socketsissa.

Proxy Serverin **Windows Sockets Servicen** avulla rajapintaa laajennetaan sallimalla sisäisessä verkossa ajettavien Windows Sockets -yhteensopivien sovellusten käyttää yhdyskäytävää ja tehdä kyselyjä internetiin. Sovellukset kuvittelevat olevansa yhteydessä internetiin, kun ne itse asiassa kommunikoivat yhdyskäytävän kanssa.

Yksi tämän suhteen kiinnostavimpia puolia on se, että asiakas voi joko käyttää IPX/SPX-protokollaa yhteydessä yhdyskäytävään, tai yhteys voi olla tavallinen TCP/IP-yhteys. IPX/SPX-protokollaa käyttävän organisaation ei tarvitse vaihtaa sisäisessä verkossa käyttämäänsä protokollaa. Vain sovelluksia, jotka on suunniteltu käyttämään Windows Socketsia TCP/IP-

yhteyden kautta, voidaan etäkäyttää näin. IPX/SPX:ää käyttävät asiakasohjelmat voivat ottaa yhteyden sisäiseen WWW-palvelimeen, jolla Proxy Serveriä käytetään tai Proxy Serveriin, joka on liitetty internetiin.

Proxy Server sisältää **Remote Windows Sockets** (RWS)-palvelun, joka vastaanottaa pyyntöjä asiakkailta ja lähettää ne edelleen proxy-palvelimelle. RWS-palvelu mahdollistaa myös proxy-palvelun välimuistiominaisuuksien käytön HTTP-, FTP- ja Gopher-resursseille. RWS-ohjelmistokomponentit voidaan asentaa asiakastietokoneelle ajamalla **Client**-hakemistossa sijaitseva SETUP-ohjelma. Asiakastietokoneen internet-selain konfiguroidaan käyttämään Proxy Serveriä.

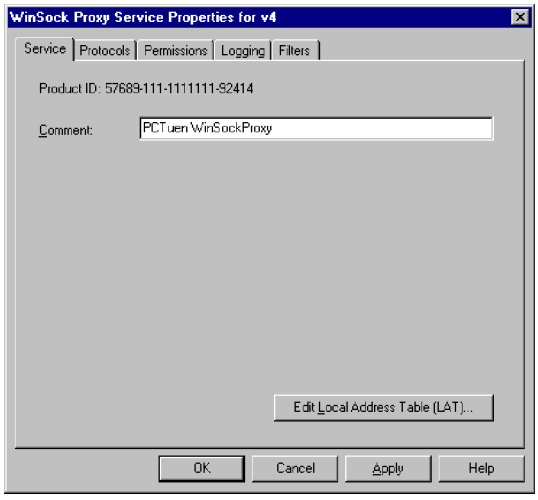
Yksityiseen sisäiseen verkkoon kuuluvia IP-osoitteita säilytetään **Local Address Tablessa** (LAT). Se luodaan Proxy Serveriä asennettaessa, ja sitä säilytetään **MSP\CLIENTS** -hakemiston tiedostona **MSPLAT.TXT**. Kun asiakastietokone määritetään käyttämään RWS:ää, taulukko noudetaan asiakkaalle ja asiakas määrittää LAT:n avulla, kuuluuko IP-osoite sisäiseen verkkoon vai internetiin. Jos osoite on internetissä, kyselyt menevät Proxy Serverille.

Palvelun asetuksissa on neljä välilehteä:

- **Service** - huomautus tai kommentti palvelusta
- **Permissions** - palvelun käyttöoikeudet
- **Logging** - pidetäänkö lokitiedostoa ja missä sitä säilytetään
- **Filters** - suodattimien määrittely.

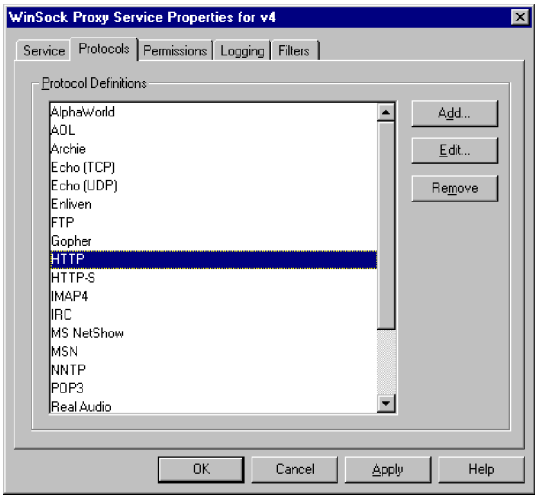
Service

Asetukset ovat seuraavat:



- **Comment** - voit kirjoittaa kommentin palvelusta
- **Edit Local Address Table** - voit muokata LAT:ia.

Protocols

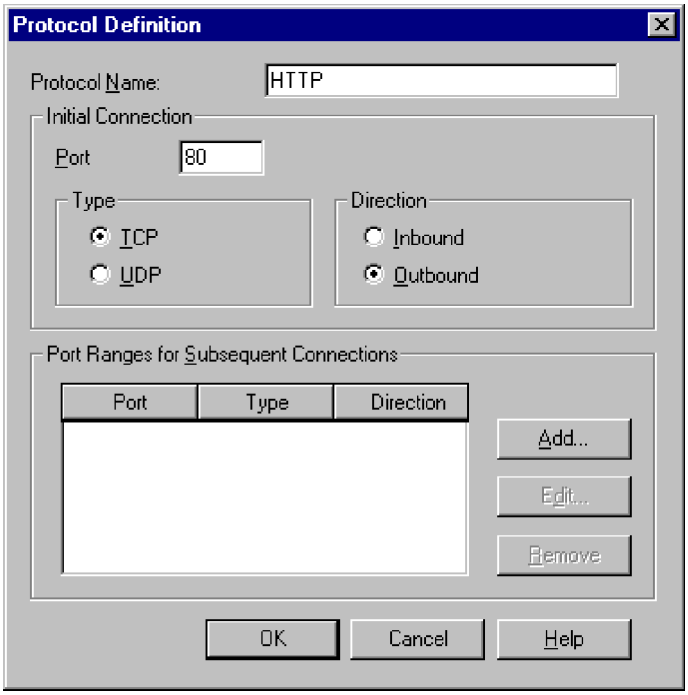


Protocols-välilehdessä voidaan asettaa käytettyjen internet-protokollien asetukset:

- **Add**-painikkeella voit lisätä oman palvelun - annettavia asetuksia ovat muun muassa nimet, porttinumerot, pakettityypit (TCP tai UDP) ja suunta (sisään tai ulos)

- **Remove**-painikkeella voit poistaa protokollan.

Edit--painikkeella voit muokata protokollan asetuksia, esimerkiksi porttinumeroa:

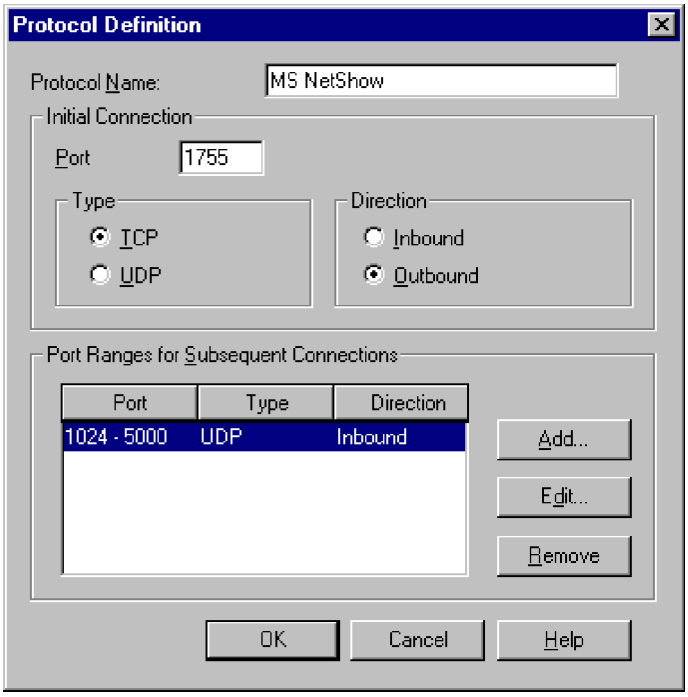


- Protocol Name on protokollan nimi

- **Initial Connection** määrittelee yhteydenoton asetukset: **Port** on portin numero, Type on tyyppi (**TCP** tai **UDP**) , Direction on portin yhteydenoton suunta (**Outbound** tai **Inbound**)

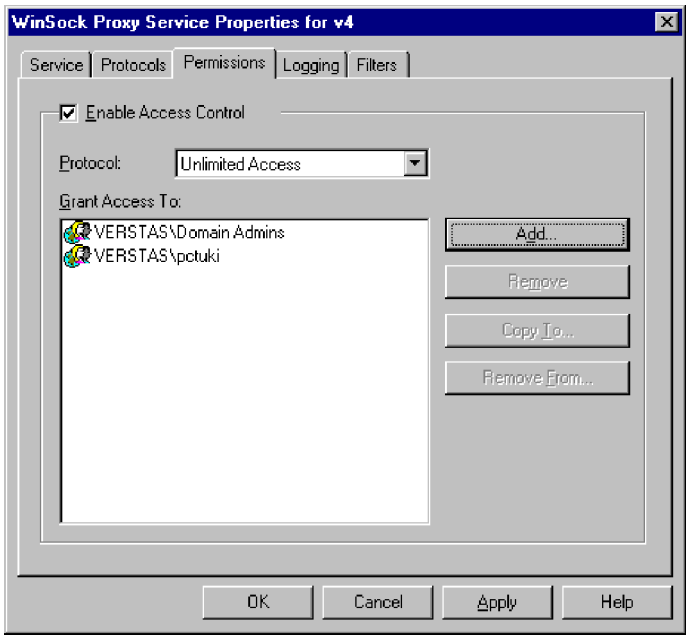
- **Port Sequences for Sequent Connections** määrittelee yhteydenoton jälkeisten porttien numerot.

Esimerkiksi MS NetShow käyttää portteja **1024 - 5000**:



Permissions

Ikkunassa voidaan ottaa käyttöoikeuksien tarkistus käyttöön (**Enable Access Control**) ja määrittää, millaiset oikeudet halutaan antaa.



- **Protocol** - valitse haluttu protokolla - **Unlimited Access** antaa oikeuden kaikkiin sovellusprotokolliin

- **Add**-painikkeella voit lisätä käyttäjätunnuksen tai -ryhmän **Grant Access To**-listaan, joita a.o. protokollan käyttöoikeus koskee

- **Remove**-painikkeella voit poistaa käyttäjätunnuksen tai -ryhmän

- **Copy to**-painikkeella voit lisätä käyttäjätunnuksen tai -ryhmän erikseen valittuun protokollaan

- **Remove From**-painikkeella voit poistaa käyttäjätunnuksen tai -ryhmän oikeuden erikseen valittuun protokollaan.

Logging

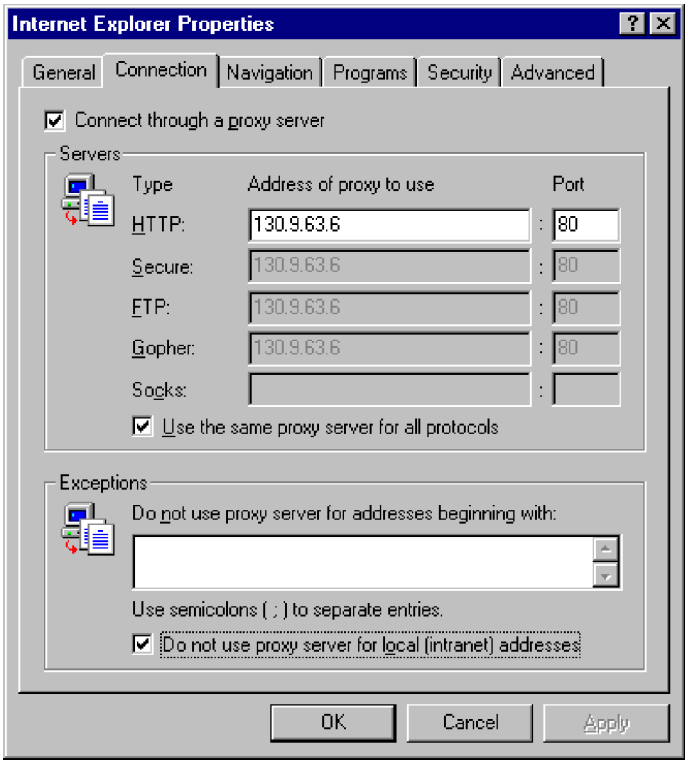
Lokit toimivat kuten Internet Information Serverin lokit, ks. asetukset IIS:n kohdalta aiemmin tässä luvussa.

Filters

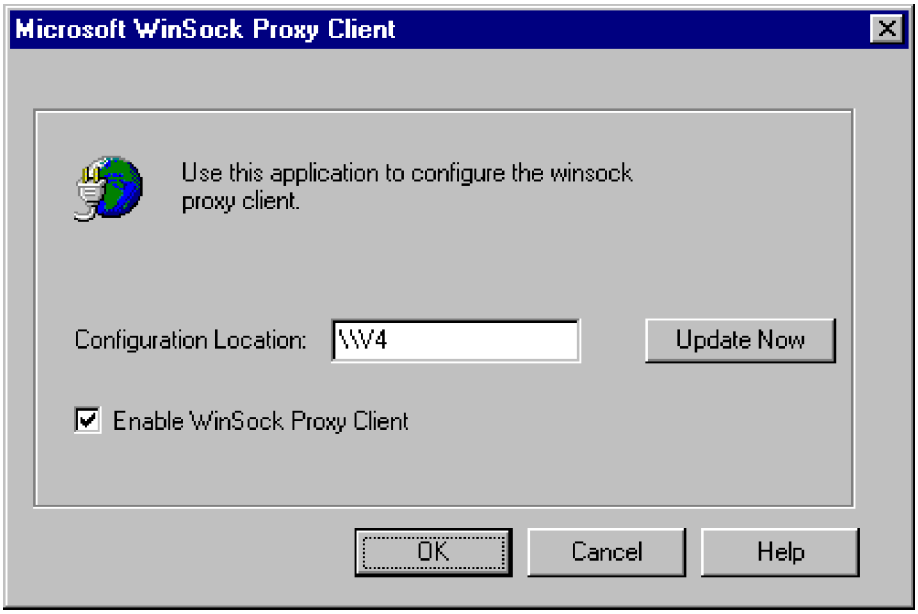
Suodattimet toimivat kuten Web Proxy Servicen lokit, ks. asetukset aiemmin tässä luvussa.

Asiakasohjelmien konfigurointi

Proxy Serveriä käyttävät asiakasohjelmat pitää asettaa pyytämään ja vastaanottamaan kohteita internetistä Proxy Serverin kautta. Asetuksen antaminen riippuu selaimesta, mutta tyypillisesti asetus tehdään **Yhteys** (Connection)-välilehdessä. Valitse **Muodosta yhteys välityspalvelimen avulla** (Connect through a proxy server). Anna Proxy Serverin osoite ja palveluiden portit. Älä käytä Proxy Serverin välityspalvelua sisäisiin osoitteisiin.



Windows Sockets -asiakasohjelmat konfiguroidaan menemällä asiakastietokoneelle ja ottamalla sitten yhteys palvelimen jaettuun **Clients**-hakemistoon. Asennusohjelma konfiguroi asiakastietokoneen automaattisesti käyttämään RWS-palvelua.



Palvelinlaajennukset

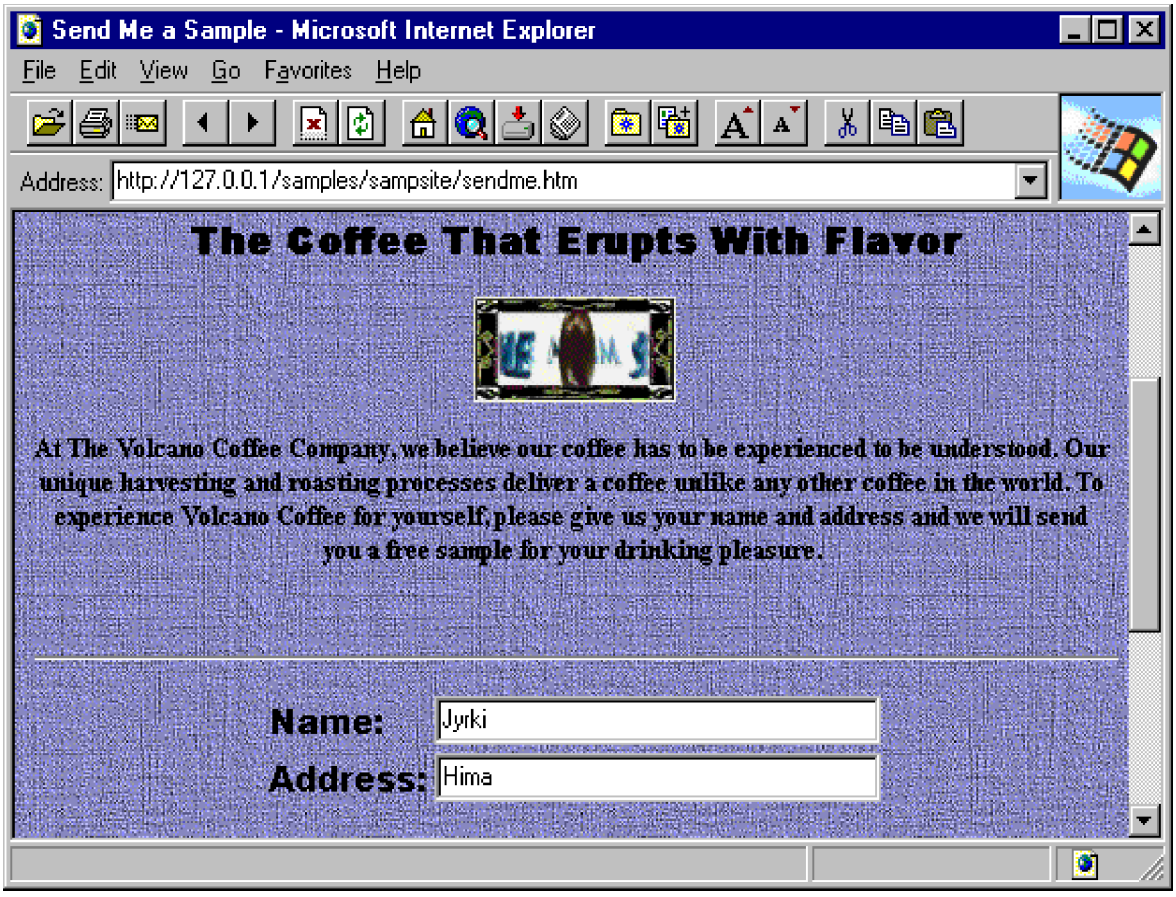
WWW-palvelimen laajennukset ovat ohjelmia, jotka toimivat WWW-palvelimessa ja toimivat vuorovaikutuksessa muiden WWW-palvelimella olevien tietojen tai ohjelmien kanssa. WWW-palvelinlaajennuksien ansiosta palvelimesta tulee dynaamisempi, ja voidaan kirjoittaa aivan uudenlaisia käyttäjien tietokoneilla toimivia ohjelmia. Java-appletit ja Microsoftin ActiveX-komponentit on suunniteltu juuri tähän tarkoitukseen.

Joulukuussa 1995 IBM:n, Microsoftin, Netscape Communicationin, Spyglassin ja Sun Microsystemsin muodostama konsortio sopi kehittävänsä yhteisen tavan, jolla aktiivisia objekteja lisätään HTML-asiakirjoihin. HTML-käskyn **<INSERT>** avulla voidaan käsitellä uusia mediatyyppejä, kuten Sunin Java-appletteja, Microsoftin COM-objekteja (*Component Object Model*), OLE-kontrolleja ja dokumentin upottamista sekä joukkoa muita Plug-inejä, joihin viitataan yleisesti **objekteina** HTML-sivuilla.

Objekti ajetaan asiakkaan tietokoneessa ja näin se siirtää osan WWW:n kuormituksesta palvelimelta. Näin voidaan tuottaa monimuotoisempaa ja aktiivisempaa sisältöä, koska palvelimen ei tarvitse käsitellä kaikkea itse.

Osa vuorovaikutteisen palvelimen mallia on luoda **dynaamisia sivuja** tietokantapalvelimilta saaduista tiedoista. Niinpä WWW-sivuilla saattaa olla vain yksi tai kaksi staattista sivua, kun taas loput luodaan dynaamisesti käyttäjien antamien tietojen pohjalta. Palvelinlaajennuksia tehdään, jotta WWW-palvelimesta saataisiin kiinnostavampi. Käyttäjälle voidaan tarjota dynaamisesti juuri haluttu tiedot, esimerkiksi säätietoja tai käyttäjän tietokannasta pyytämiä tietoja.

Lähin esimerkki saattaa olla **Volcano Coffee Companyn** mallilomakkeet. **Volcano Coffee Company** on WWW-mallipalvelin, joka tulee Microsoft Internet Information Serverin mukana.



Jos täytät mallilomakkeen, näet seuraavanlaisia tekstejä selaimesi tilarivillä painaessasi **Submit**-painiketta:

http://127.0.0.1/scripts/samples/volresp.dll?name=Jyrki&address=Hima&type=Mo%27a+Mana+Blend

Se on lomakekoodia, ja ylläoleva koodinpätkä lähetetään WWW-palvelimelle. Huomaa, että palvelimen osoite on URL:ssä, samoin kuin lomakkeella annetut nimi- ja tuotetyyppitiedot (tässä esimerkissä kysymykses-

sä on **localhost**). Kysymysmerkin jälkeen tuleva teksti välitetään syötteeksi skriptille tai ohjelmalle. Plus- ja &-merkit erottavat tiedon sanoja ja kenttiä. Ohjelmien on osattava lukea ja käyttää lomakkeen tietoja.

Internet Information Serverissä voit käyttää lähes mitä tahansa 32-bittistä ohjelmointikieltä vuorovaikutteisten ohjelmien tekemiseen jommallekummalle IIS:n rajapinnalle:

- **CGI** (*Common Gateway Interface*)
- **ISAPI** (*Internet Server API*).

Common Gateway Interface

Tavallisin tapa tehdä palvelinlaajennuksia on ollut kirjoittaa **Common Gateway Interface** (CGI)-skriptejä. WWW-sivu keräsi käyttäjältä tietoja, kuten esimerkiksi nimen ja osoitteen, tallensi sitten tiedon myöhempää käyttöä varten tai kehitti tietojen pohjalta heti toisen lomakkeen.

CGI-rajapinta on protokolla, joka mahdollistaa WWW-asiakasohjelmien ja WWW-palvelinten välisen kaksisuuntaisen liikenteen rajapinnan kautta. CGI-skriptit taas ovat joukko käskyjä, jotka määrittelevät, mitä tapahtuu, kun ne kommunikoivat. CGI kehitettiin HTTP-protokollan laajennukseksi.

IIS:n WWW-palvelussa toimivat vain 32-bittiset CGI-sovellukset. Lisäksi käyttäjät, jotka kirjautuvat käyttämällä **Windows NT Challenge/Response** -protokollaa, **eivät** voi suorittaa CGI-skriptejä.

CGI määrittelee seuraavat asiat:

- HTML-asiakirjoihin sijoitettavat CGI-ohjauskäskyt ja kenttätarkenteet
- Muistin ympäristömuuttujan, jonne palvelin sijoittaa skriptien käyttämät tiedot
- Asiakkaan, palvelimen ja skriptin välisen tiedonsiirron.

CGI:n käyttö aloitetaan luomalla ensin HTML-lomake, jossa on CGI-käskyjä. Käskyt määrittelevät lomakkeilla näkyvät syöttökentät, avattavat luetteloruudut ja painikkeet, jotka keräävät käyttäjien syötteen. Käskyt

määrittelevät myös syötteen vastaanottotavan ja sitä käsittelevän CGI-skriptin nimen.

Seuraavaksi tarvitaan **CGI-skripti**. Se voi olla millä tahansa ohjelmointikielellä kirjoitettu ohjelma. Ainoa, mitä ohjelmalta vaaditaan on, että se hyväksyy standardin ASCII-tekstitiedon, jonka käyttäjä on kirjoittanut HTML-lomakkeeseen, ja osaa tehdä sille jotain. Ohjelma voi esimerkiksi antaa jonkinlaisen tulosteen tai tuloksia, jotka voidaan sijoittaa toiseen HTML-asiakirjaan, joka lähetetään takaisin käyttäjälle.

Palvelimella suoritettava HTTP-protokolla tietää, mitä sen pitää tehdä CGI-lomaketietojen kanssa edellyttäen, että lomake on oikein koodattu. Käyttäjä täyttää lomakkeen ja lähettää sen takaisin palvelimelle. Palvelin vastaanottaa tämän tiedon, joka sisältää CGI-skriptin nimen ja sitten se yksinkertaisesti lähettää ASCII-tekstitiedon skriptille palautuslomakkeella.

Skripti vastaanottaa tiedon syötteenä ja tekee sille jotain: jos tieto on esimerkiksi nimi- ja osoitetietoja, se saattaa vain liittää sen tekstitiedostoon tai tietokantaan. Se saattaa myös käyttää annettua syötettä etsimään muuta tietoa tietokannasta ja palauttaa sen jälkeen tulokset WWW-asiakasohjelmalle.

Tietoturvallisuuden kannalta on riskialtista antaa käyttäjien ajaa CGI-ohjelmia. Skriptit pitäisi suorittaa vain niissä hakemistoissa, joissa on suoritusoikeus. **Internet Information Server** luo **\Scripts** -hakemiston, jolla on suoritusoikeus; CGI- ja ISAPI-ohjelmat pitäisi asentaa tähän hakemistoon. Kun hakemistossa on vain suoritusoikeus, käyttäjät eivät voi siirtää sinne ohjelmia eivätkä käyttää ohjelmia, jotka saattavat sisältää viruksia. Vain pääkäyttäjät voivat lisätä ohjelmia hakemistoon, missä tietysti siinäkin piilee tietoturvallisuusriski:

- Kaikki ohjelmien käynnistämät prosessit tulisi suorittaa käyttäjätunnuksin, joilla on riittävät (mutta ei sen enempää) käyttöoikeudet. Jos ohjelma käsittelee tiedostoja tai kirjoittaa tiedostoihin, sillä on oltava NTFS-tiedostojärjestelmän oikeudet käyttää tiedostoja. Yleensä nämä oikeudet annetaan tunnukselle, jota käytetään ohjelmien suorittamiseen (esimerkiksi System)

- Ohjelmat, jotka eivät tarvitse käyttäjän antamia tietoja, voidaan suorittaa yksinkertaisen HTML-tiedostossa olevan linkin kautta. Käyttäjä napsauttaa painiketta, joka viittaa URL-osoitteeseen, ja siinä on määritelty suoritettavan ohjelmatiedoston sijainti ja nimi. Yleensä URL kutsuu **\Scripts**-hakemistoon sijoitettua suoritettavaa ohjelmaa

- Jos haluat kerätä tietoja käyttäjiltä, laita HTML-asiakirjoihisi HTML-lomakekomponentteja

- CGI-ohjelmia voidaan tehdä millä tahansa kielellä, mutta on ehkä määriteltävä Internet Information Serverille, mikä kääntäjä sen on kytkettävä käyttämääsi kieleen. Kytkennän määrää tiedoston tarkennin. Tunnettuja tarkentimia ovat mm. .EXE, .COM, .BAT, .CMD, .DLL, .IDC (*Internet Database Connector*) ja .PL (*Perl*).

Internet Server API

CGI ei kuitenkaan ole kovin tehokas kuormitetuilla palvelimilla. **Internet Server API** (ISAPI) tarjoaa paremman suorituskyvyn ja voi palvella useampia palvelimia kuin CGI-sovellukset. ISAPIn ominaisuuksiin kuuluvat muun muassa:

- Sisäänrakennettu tuki räätälöityjen CGI-laajennusten tekemiseen

- **ISAPI Application Interface**, joka on periaatteessa CGI:n tehokkaampi versio. Siinä on mukana laajennuksia ja se käyttää dynaamisia linkkikirjastoja (*Dynamic Link Library*, DLL). DLL ladataan palvelimen muistiin, ja siitä tulee osa palvelinsovellusta. Näin saavutetaan merkittävän tehonlisäys, ja ohjelmankehityksen näkökulmasta DLL on helppo luoda. Muistimallien, segmenttien ja muiden "vanhojen" ohjelmointitekniikoiden kanssa ei välttämättä tarvitse olla tekemisissä. DLL:t pysyvät lataamisen jälkeen muistissa, kunnes palvelu lopetetaan tai palvelin poistaa ne muistista

- **ISAPI Filter API**, joka mahdollistaa millaiset tahansa ISAPIn laajennukset, joiden avulla voidaan käsitellä vapaasti HTTP-pyyntöjä ja -vasteita

- **Internet Database Connector**-tuki, joten voit kytkeä WWW-palvelimen ODBC-tietolähteisiin.

Volcano Coffee Companyn mallisivuilta näkee miten ISAPI DLL:t on integroitu IIS:n WWW-palvelimeen. Jos esimerkiksi haluat nähdä, kuinka tieto poimitaan lomakkeelta ja käytetään DLL:n syötteenä, avaa HTML-asiakirja:

http://127.0.0.1/samples/sampsite/sendme.htm

Kun katsot tämän HTML-asiakirjan lähdettä, huomaat rivin, joka lähettää WWW-asiakasohjelman syötteen **VOLRESP.DLL**-tiedostolle:

<FORM action="/scripts/samples/volresp.dll">

ActiveX Server Framework on ISAPIn lisäys, joka tarjoaa aktiiviset palvelinkontrollit sekä skriptit. Sen avulla ohjelmoijat voivat luoda WWW-sovelluksia, joissa on uudelleen käytettäviä komponentteja. Koska olemassa olevat OLE-komponentit sopivat myös tähän malliin, ohjelmoijat voivat hyödyntää jo tekemiään OLE-komponentteja. Skriptit tarjoavat ympäristön aktiivisten palvelinkomponenttien ajamiseen ja komponenttien yhteenliittämiseen.

Microsoft Visual Basic Scripting Edition

Microsoftin tavoitteena on luoda kehitysympäristö, jossa sovellusten ja WWW-sivujen yhteiset komponentit liitetään yhteen yhteisellä skriptikielellä. Sen ohjelmakomponenttiarkkitehtuuri on kieliriippumaton, mikä tarkoittaa sitä, että komponentteja voidaan tehdä C:llä, Visual Basicilla tai Javalla. Skriptikieli on suunniteltu koordinoimaan komponentteja ja muokkaamaan niiden toimintaa.

Microsoftin ensijainen skriptikieli on Visual Basic Scripting Edition (VBScript), vaikka se ei suljekaan pois Javan tai C++:n käyttöä. Skriptejä voidaan kirjoittaa millä tahansa näistä. VBScriptillä voidaan tehdä eläviä, aktiivisia, mielenkiintoisia ja älykkäitä WWW-sivuja, jotka osaavat vastata kysymyksiin ja kyselyihin, tehdä kysymyksiä, tarkistaa käyttäjätietoja, laskea lausekkeita, linkittyä toisiin sovelluksiin sekä yhdistää OLE-kontrolleihin, appletteihin ja kolmiulotteisiin animaatioihin.

VBScriptin ominaisuudet käsittävät mm. seuraavat:

- WWW-selainten skriptaus-, automatisointi- ja muokkausominaisuudet
- VBScript on Visual Basic -kielen yksinkertaisempi, yhteensopiva versio
- VBScript on optimoitu internet-selaimille ja -palvelimille
- VBScript-koodi on HTML-asiakirjassa olevaa ASCII-tekstiä, joka käännetään, kun tiedosto ladataan.

VBScriptiä voidaan käyttää sekä selaimen että muiden työpöydällä olevien sovellusten käsittelemiseen. Sillä voidaan myös ohjata HTML-sivulla olevia OLE-kontrolleja ja Java-appletteja.

VBScript-koodi lisätään HTML-asiakirjoihin muotoilukäskyjä käyttäen. **<Language=VBS>**:ksi määritelty **<Script>**-niminen muotoilukäsky kertoo selaimelle, että kaikki, mitä on käskyjen **<Script>** ja **</Script>** välissä, pitää käsitellä VB-skriptinä. VB-skriptitulkki integroidaan **ActiveX Scripting** -määrityksen rajapintoja käyttämällä.

Microsoft jakaa VBSciptiä ilmaiseksi, mutta kaikki selainvalmistajat eivät tue sitä. Microsoftin Internet Explorer ja Oraclen, Spyglassin, NetManagen ja muiden Microsoftin internet-alustan lisensoineiden valmistajien selaimet tukevat VBScriptiä.

ActiveX

ActiveX-komponentit ovat ohjelmakomponentteja, jotka toimivat internetissä, intraneteissä tai yksittäisissä tietokoneissa. Ne ovat aktiivisen sisällön internet-käyttöön optimoituja rakennuspalikoita. Active-skriptien avulla ohjelmoijat liittävät nämä rakennuspalikat WWW-sovelluksiin. Active-skriptejä voidaan tehdä Visual Basic-, Scripting Edition- ja JavaScript-yhteensopivilla menetelmillä.

Active Server Pages

Internet Information Server 3.0 versiossa on mukana **Active Server Pages** ominaisuus, jonka avulla WWW-sivujen tekijät voivat yhdistää HTML:ää skriptikirjoitukseen lähes kaikilla välineillä. Skripteissä voidaan viitata paikallisella tai millä tahansa palvelimella ajettaviin komponentteihin, joiden avulla voidaan käyttää tietokantoja, sovelluksia tai käsitellä tietoja.

Kun selain pyytää ASP-tiedostoa, se käsitellään palvelimella ja sivu palautetaan asiakkaalle standardi-HTML:nä.

Kehittäjien ei tarvitse IIS 3.0:aa käyttäessään käyttää mitään tiettyä skriptikieltä WWW-sovellusten luomiseen, koska Active Server Pages sivut ovat yhteensopivia kaikkien ActiveX-skriptikielten kanssa. Active Server Pages sisältää tuen **Visual Basic** skriptikielelle (VBScript) ja **JScriptille**. Lisäksi on saatavilla erillisiä plug-inejä, jotka tarjoavat tuen muille kielille, esimerkiksi REXX:ille, Perlille ja Tcl:lle. Eri skriptikieliä voidaan käyttää jopa samassa ASP-tiedostossa.

ActiveX-palvelinkomponentteja voidaan luoda käytännössä millä tahansa kielellä, esimerkiksi Javalla, Visual Basicilla, C++:lla ja COBOL:illa.

HTML-sivujen tekijöiden on Active Server Pagesin avulla helppo *aktivoida* WWW-sivunsa palvelimella. Räätälöidyt sivut ja yksinkertaiset sovellukset voidaan kehittää välittömästi. Käyttäjän mukaan räätälöidyn sisällön luomiseen ei tarvita monimutkaisia Perl- tai C-kielellä kirjoitettuja CGI-ohjelmia, vaan kaikki voidaan tehdä Active Server Pagella. Seuraavassa yksinkertaisessa esimerkissä käytetään VBScriptiä näyttämään kellonaika ja asiakkaan käyttämän selaimen tyyppi:

```
<HTML>
<HEAD>
<TITLE>WWW-esimerkkisivu</TITLE>
</HEAD>
<BODY>
<P>
Hei <%= Request.ServerVariables( REMOTE_USER ) %>
Kello on <%= now%>
Selainohjelmasi on <%=Request.ServerVariables( http_user_agent ) %>
</BODY></HTML>
```

Active Server Pages tarjoaa sovellussuunnitteluun selaimista riippumattoman lähestymistavan. Koska koko dynaamisen sisällön luomiseen tarvittava sovelluslogiikka voidaan ajaa palvelimella, suunnittelijoiden ei tarvitse välittää siitä, mitä selainta sivujen katseluun käytetään - selaimen kannalta ASP-tiedosto on tavallinen HTML-sivu.

Active Server Pages tekee skriptauksella ja komponenttien käytöllä mahdolliseksi tietokantojen ja sovellusten käyttöön tarvittavan ohjelmoinnin erottamisen WWW-sivun suunnittelusta ja muusta sisällöstä. Näin voidaan varmistaa, että kehittäjät (*Developer*) tai ohjelmoijat (*Programmer*) voivat keskittyä komponenttien kirjoittamiseen ilman, että heidän tarvitsee huolehtia siitä, miltä lopputulos näyttää. Varsinaiset WWW-sivujen suunnittelijat (*Designer*) voivat taas keskittyä sivun ulkonäön suunnitteluun ja he voivat muuttaa sivun ulkonäköä tuttujen välineiden avulla.

IIS ja DCOM

ASP-pohjaisen sovelluksen muodostavat komponentit ajetaan tavallisesti samassa prosessissa kuin IIS 3.0, jolloin tehokkuus on parhaimmillaan. Sovellukset kommunikoivat keskenään ja palvelimen kanssa **Component Object Modelin** (COM) kautta. Kun sovellukset muuttuvat monipuolisemmiksi, komponentteja halutaan suorittaa ajaa eri palvelimilla ja asiakkailla. Tämä on mahdollista Distributed COM:in (DCOM, jaettu COM) avulla. DCOM hoitaa kaikki etäkutsut, jolloin kehittäjät voivat käyttää samaa koodia riippumatta siitä, missä objektia ajetaan. Komponenttien välinen tiedonsiirto hoidetaan saman rajapinnan kautta.

Microsoft Transaction Server

Kun organisaatiot siirtyvät yhä enemmän käyttämään komponenttipohjaisia sovelluksia WWW:ssä, tarvitaan menetelmä, jolla voidaan helposti päivittää sovelluksia sekä saada järjestelmään tuki tapahtumien (*transaction*) käsittelylle.

Microsoft Transaction Server (*Viper*) tarjoaa komponenttipohjaisille sovelluksille automaattisen tapahtumatuen. Tällöin voidaan sekä rakentaa että muuttaa nopeasti palvelinsovelluksia ilman, että luotettavuutta ja laajennettavuutta menetettäisiin. Active Server Page -sovellukset voidaan liittää suoraan Transaction Serveriin.

Transaction Server -palveluita ovat esimerkiksi käyttöjärjestelmäprosessien ja säikeiden hallitseminen, palvelinprosessien hallinta, resurssien käytön synkronointi useiden asiakaspyyntöjen kesken sekä keskitetty ylläpito ja konfigurointi.

Java ja JavaScript

Java on tehokas työkalu, jolla voidaan tehdä internetissä toimivia asiakas/palvelin-sovelluksia. Java on todennäköisesti ensimmäinen kieli, joka on suunniteltu verkkoympäristöön. Arkkitehtuuriin kuuluu asiakkaaseen sisältyvä Java-tulkki, joka on Javan laitteistoriippumattomuuden perusta. Kaikille tärkeimmille käyttöjärjestelmille on tarjolla oma tulkkinsa. Java-appletit lähetetään ohjeina, jotka käännetään nopeasti käyttäjän koneessa ajettaviksi ohjelmiksi.

Ennen tietojen siirtämistä Java selvittää selaimelta, onko järjestelmässä Java-tulkki. Jos sitä ei ole, näytölle ilmestyy kuva tai teksti, jossa käyttäjältä kysytään haluaako hän kopioida tulkin koneelleen. Koska tulkit on suunniteltu kullekin käyttöjärjestelmälle erikseen, WWW-palvelimille tallennettujen Java-applettien pitäisi toimia samalla tavalla käytettävästä laitteistosta riippumatta.

Yksi haittapuoli ohjelmien kopioimisessa toisesta koneesta on, että ohjelmissa saattaa olla virus. Java-appletit pyrkivät kiertämään tämän ongelman niin, että ne eivät anna ohjelman käyttää mitä tahansa muistipaikkoja.

Lisätietoja Javasta löydät Sunin Java-sivuilta osoitteesta **http://java.sun.com**.

Open Database Connectivity

Open Database Connectivitystä (ODBC) on tullut tietokantahakujen teollisuusstandardi. Se on toimittajariippumaton, ja Microsoft on yhdessä **ANSI**n (*American National Standards Institute*), SQL Access Groupin, X/Openin ja riippumattomien ohjelmistotoimittajien kanssa pyrkinyt tekemään siitä avoimen standardin.

ODBC:stä on hyötyä sekä ohjelmoijille että käyttäjille. Sen avulla käyttäjät voivat hakea tietoja yhden sovelluksen avulla silloinkin, kun tieto on varastoitu eri paikkoihin ja erilaisiin tietokantajärjestelmiin, kuten **DB2**, **ORACLE**, **DEC RDB**, **Apple DAL**, **dBASE** ja **Microsoft SQL Server**. ODBC yksinkertaistaa sovelluskehitystä, ja tietoja voidaan hakea useista tietokannoista samanaikaisesti. Samaa liittymää ja hakumenetelmiä voidaan käyttää eri alustoilla, ja sovellukset voidaan eristää taustalla olevien verkon ja tietokannan hallintajärjestelmien (**DBMS**) versiomuutoksilta. ODBC tukee SQL:n käyttöä.

ODBC toimii työasemasovellusten ja palvelinohjelmistojen välillä olevan ohjelmointirajapinnan (API) kautta. Se muodostaa kerroksen, joka osaa piilottaa niiden väliset erot. Työasemasovellukset voivat käyttää samaa koodia keskustellessaan monien erityyppisten tietolähteiden kanssa.

Internet Database Connector toimitetaan Microsoft Internet Information Serverin mukana. Se on **HTTPODBC.DLL**-niminen dynaaminen linkkikirjasto (DLL), joka mahdollistaa ODBC:n kautta useiden tiedonhallintaohjelmistojen käytön. IDC toimii WWW-palvelimen ja ODBC-rajapinnan välillä. IDC muodostaa linkit WWW-asiakasohjelmien sekä Microsoft SQL Serverin ja muiden vastaavien relaatiotietokantapalvelinten välille.

Jos käytössäsi on SQL Server, niin pääset heti tutustumaan IDC-tekniikkaan. Internet Information Serverin mukana tulee joukko WWW-mallisivuja, joissa on näytetty, kuinka tietokantaliittymä voidaan toteuttaa. Voit tarkastella HTML-sivujen lähdekoodia sekä .IDC- ja .HTX-tiedostoja.

Microsoft FrontPage

FrontPage on työkalu, joka on tarkoitettu nimenomaan WWW-julkaisemiseen ja monimutkaisten WWW-sivukokonaisuuksien kehittämiseen. Yksi FrontPagen ja esimerkiksi Internet Assistantin suurimmista eroista on se, että FrontPage on suunniteltu jaettuihin, monen käyttäjän työympäristöihin. Tämä tarkoittaa, että se on suunniteltu WWW-aineistoa kehittävien työryhmien ja tiimien apuvälineeksi.

Koska FrontPage on monen käyttäjän työväline, sen käyttöliittymä ja arkkitehtuuri on suunniteltu siten, että WWW-sivujen ulkoasun suunnittelijat voivat työstää aineistoa omalla työasemallaan tai internetissä.

FrontPagesta on saatavilla sekä Macintosh- että Windows-versiot, mutta koska se tuottaa standardeja HTML-asiakirjoja, valmis aineisto voidaan tallentaa sekä Windows NT-, Windows 95-, Macintosh- että UNIX-pohjaisille WWW-palvelimille.

FrontPagessa on kaksi tärkeää osaa:

- FrontPage Explorer on työkalu, jolla WWW-palvelinta ja kehitystiimisi luomaa sivukokonaisuutta pidetään yllä

- FrontPage Editorilla kehittäjäsi voivat luoda ja muokata WWW-sivuja.

Kehitysprosessissa käytettäviä lisäkomponentteja on mm. **To Do List**, joka on väline käyttäjien ja heidän tehtäviensä seurantaan, sekä **WebBo**-**t**it, jotka ovat WWW-sivujen vuorovaikutteisia toimintoja. WebBoteilla voidaan automatisoida tehtäviä ilman ohjelmointia.

FrontPagessa on myös koko joukko ohjattuja toimintoja, jotka automatisoivat joitakin WWW-sivujen luontiin liittyviä tehtäviä, sekä mallipohjia, joita käyttämällä on helppo luoda WWW-sivuja ennalta tehtyjen asetusten mukaan.

FrontPage sisältää myös oman palvelimen, joka toimii Windows 95- ja Windows NT -koneissa. Vaikka se ei sisälläkään kaikkia Internet Information Serverin piirteitä ja tietoturvaominaisuuksia, sitä voi käyttää kevyenä palvelimena testattaessa WWW-sivuja. Käyttäjät voivat myös käyttää sitä sisäisessä verkossa halutessaan julkaista omia WWW-sivujaan.

10. REKISTERI

Windows NT:n rekisterin perusteita on käsitelty Windows NT 4.0 Tehokäyttäjän Opas Osa 1:ssä.

Tässä kirjassa rekisterivinkit on pyritty sijoittamaan sinne, minne ne loogisesti kuuluvat.

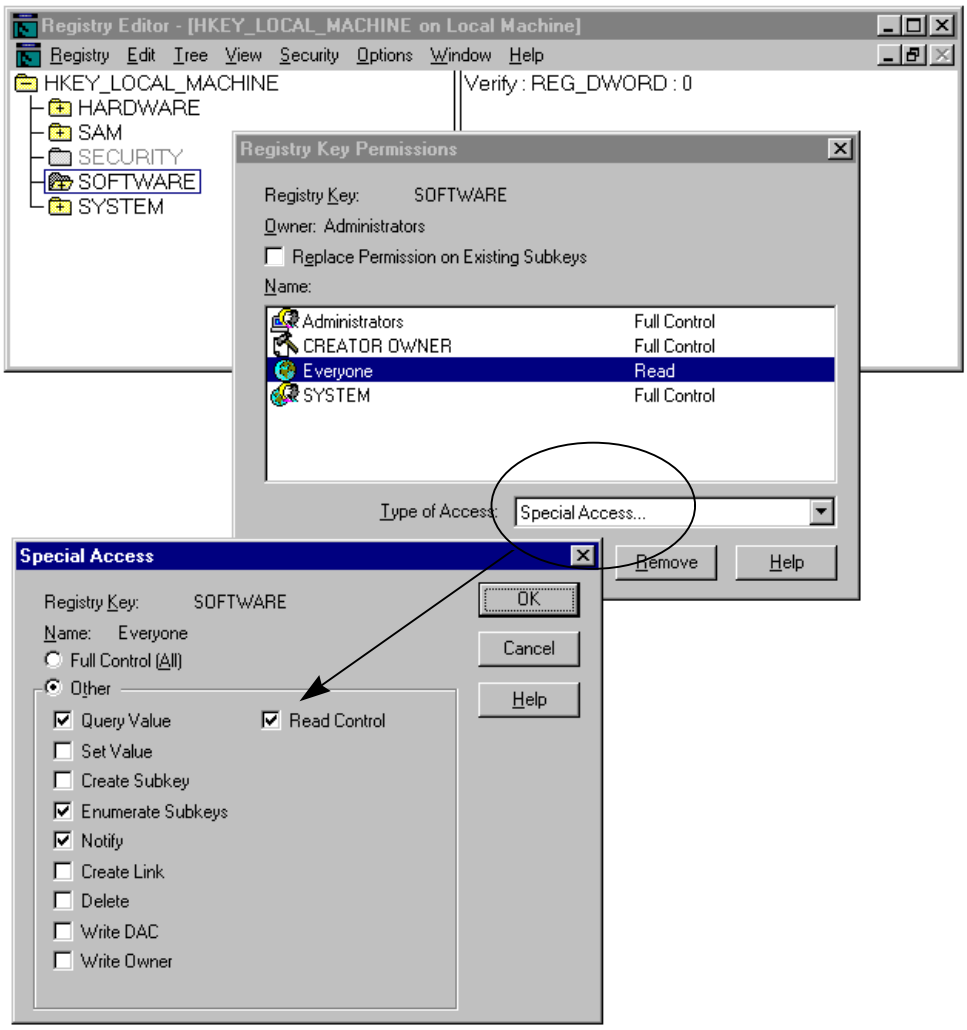
Tässä luvussa käsitellään rekisterin suojauksia ja lyhyesti apuohjelmia rekisterin käsittelyyn.

Rekisterin suojaukset

Viimeaikoina raportoidut Windows NT:n murtautumisyritykset ovat paljolti perustuneet rekisterin puutteellisiin suojauksiin, mikä on mahdollistanut rekisteriin käsiksi pääsyn verkon kautta tai paikallisesti. Jos haluat lisätä NT:n rekisterin suojauksia, voit tehdä seuraavat muutokset rekisterin käyttöoikeuksiin. Ole varovainen!

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify, Read Control**

Tällä asetuksella määritellään kuka saa asentaa ohjelmistoja NT-koneeseen. **Älä** anna asetusta aliavaimiin!



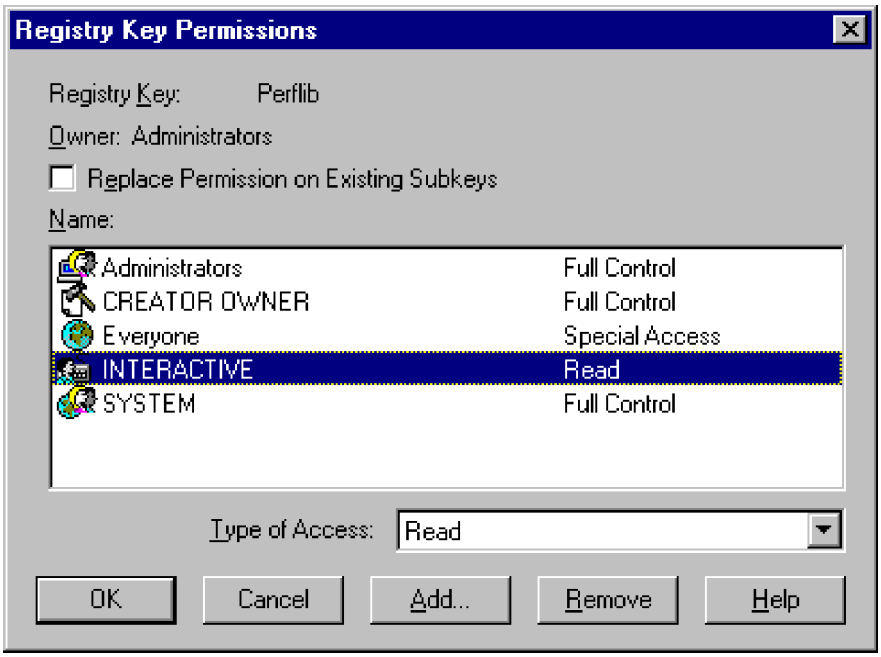
RPC-palveluiden lukitseminen - anna myös aliavaimiin:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\RPC**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify, Read Control**

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion** **\Microsoft\Windows NT\CurrentVersion\Profile List** **\Microsoft\Windows NT\CurrentVersion\AeDebug** **\Microsoft\Windows NT\CurrentVersion\Compatibility** **\Microsoft\Windows NT\CurrentVersion\Drivers** **\Microsoft\Windows NT\CurrentVersion\Embedding** **\Microsoft\Windows NT\CurrentVersion\Fonts** **\Microsoft\Windows NT\CurrentVersion\FontSubstitutes** **\Microsoft\Windows NT\CurrentVersion\Font Drivers** **\Microsoft\Windows NT\CurrentVersion\Font Mapper** **\Microsoft\Windows NT\CurrentVersion\Font Cache** **\Microsoft\Windows NT\CurrentVersion\GRE_Initialize** **\Microsoft\Windows NT\CurrentVersion\MCI** **\Microsoft\Windows NT\CurrentVersion\MCI Extensions**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify, Read Control**

Tämä asetus määrittelee, kuka saa seurata NT-koneen suorituskykyä. Poista Everyonelta Read-oikeus, ja voit antaa sen vuorovaikutteiselle käyttäjälle (käyttäjä, joka on kirjautunut paikallisesti):

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\PerfLib**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify** **INTERACTIVE: Read**



Anna myös oikeus kaikkiin aliavaimiin:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Port**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Type1 Installer**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Anna myös oikeus kaikkiin aliavaimiin:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\WOW**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Anna myös oikeus kaikkiin aliavaimiin:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion \Windows3.1MigrationStatus**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**CurrentControlSet\Services\LanmanServer\Shares**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Huomaa, että myös mahdollisesti UPS-palvelulle määritelty komentojono on suojattava! Administrators ja System: Full Control.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**CurrentControlSet\Services\UPS**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

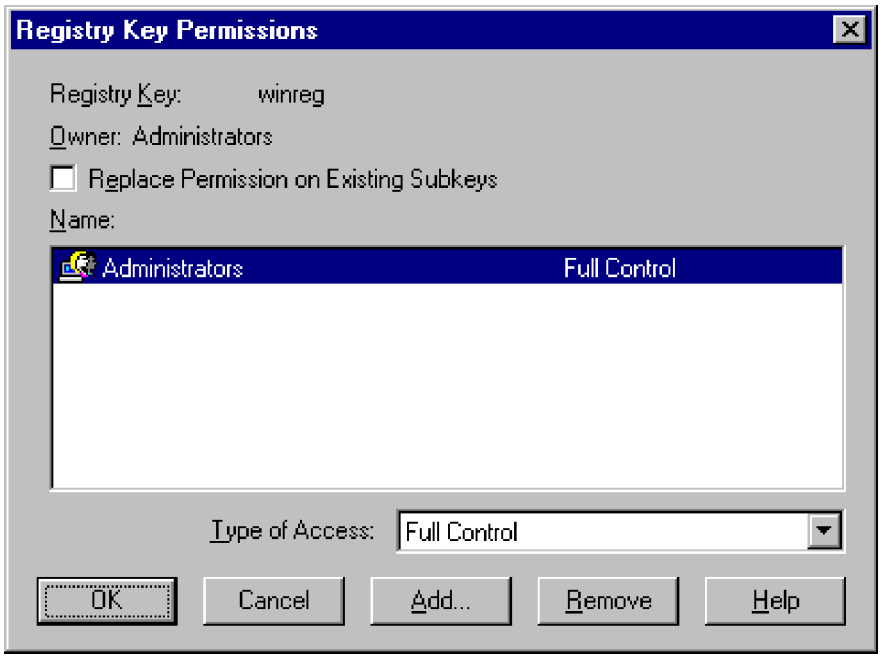
Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**CurrentControlSet\Services\UPS**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Polku	**HKEY_CLASSES_ROOT**
Avain	**kaikki aliavaimet**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Polku	**HKEY_USERS**
Avain	**\.DEFAULT**
Oikeus	**Everyone: QueryValue, Enumerate Subkeys, Notify**, **Read**

Seuraava asetus määrittelee oikeudet verkon kautta rekisteriin.NT-työasemassa asetusta ei ole oletuksena, NT-palvelimessa oikeus on vain vain pääkäyttäjillä (Administrators-ryhmä). Anna rajoituksia tarpeen mukaan. Myös monistuspalvelun käyttäjätunnukselle olisi annettava tämä oikeus (voit myös tarkistaa, ettei monistuspalvelun käyttäjätunnuksella ole oikeutta kirjautua paikallisesti palvelimelle (Log on Locally).

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentcontrolSet\Control\SecurePipeServers\winreg**
Oikeus	**Administrator: Full Control**



Apuohjelmia rekisterin käsittelyyn

Windows NT 4.0:n suosion myötä on alkanut iklmestyä yhä enemmän apuohjelmia myös rekisterin käsittelyyn, mutta myös vanhat konkarit päivittävät omia versioitaan: etsi uusimmat versiot esimerkiksi näistä internetin hakukoneilla:

- ISES Registry Class Browser
- ISES Registry Surfer
- Somarsoft: DumpAcl shareware registry utility.
- Somarsoft: DumpEvt shareware event log utility.
- Somarsoft: DumpReg shareware registry utility.
- Somarsoft: RegEdit shareware registry DLL.
- Registry Search and Replace (Steven J. Hoek)

Hyviä osoitteita ovat esimerkiksi:

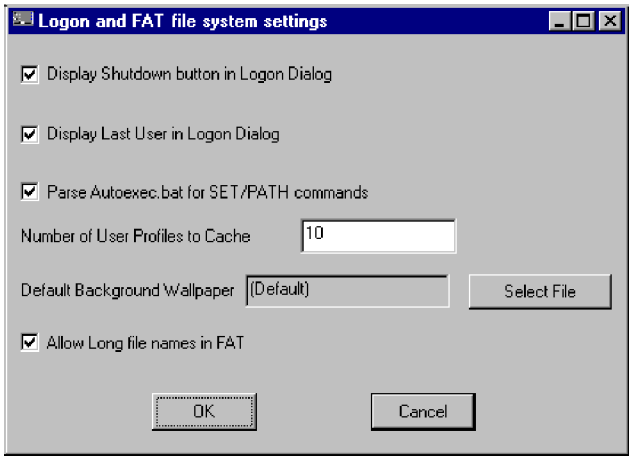
- http://www.bhs.com
- http://www.winntmag.com
- http://www.shareware.com
- http://www.ntinternals.com.

Tietysti myös Resource Kitin mukana tulee joukko rekisteriin käsittelyyn tarkoitettuja apuohjelmia.

REGBACK.EXE - ottaa varmistuksen rekisterin avaimesta, joka on auki! XCOPY-komennolla voit varmistaa loput.

REGKEY.EXE - antaa mahdollisuuden määritellä Shutdown-nappulan, vimeisen kirjautuneen käyttäjän tunnuksen näyttämisen, pitkät tiedostonimet FAT-levyllä jne

REGREST.EXE - mahdollisuus palauttaa rekisterin tiedostot



REGSEC.EXE - suojaa rekisterin

COMPREG.EXE - mahdollistaa kahden NT-koneen rekisterien vertaamisen

DELSRV.EXE - poistaa palvelun (Service)

REGCHG.EXE - rekisterin asetusten muutos paikallisessa tai etäkoneessa

REGDEL.EXE - poistaa rekisterin avaimen paikallisessa tai etäkoneessa

REGINI.EXE - mahdollistaa rekisterin asetusten muutoksen scriptin avulla

REGREAD.EXE - lukee rekisterin asetuksia näytölle

RESTKEY.EXE - rekisterin avaimen palautus tiedostosta

RREGCHG.EXE - muuttaa etäkoneen rekisterin asetuksia

SAVEKEY.EXE - tallentaa rekisterin asetuksia tiedostoon

SCANREG.EXE - merkkijonojen etsiminen rekisteristä

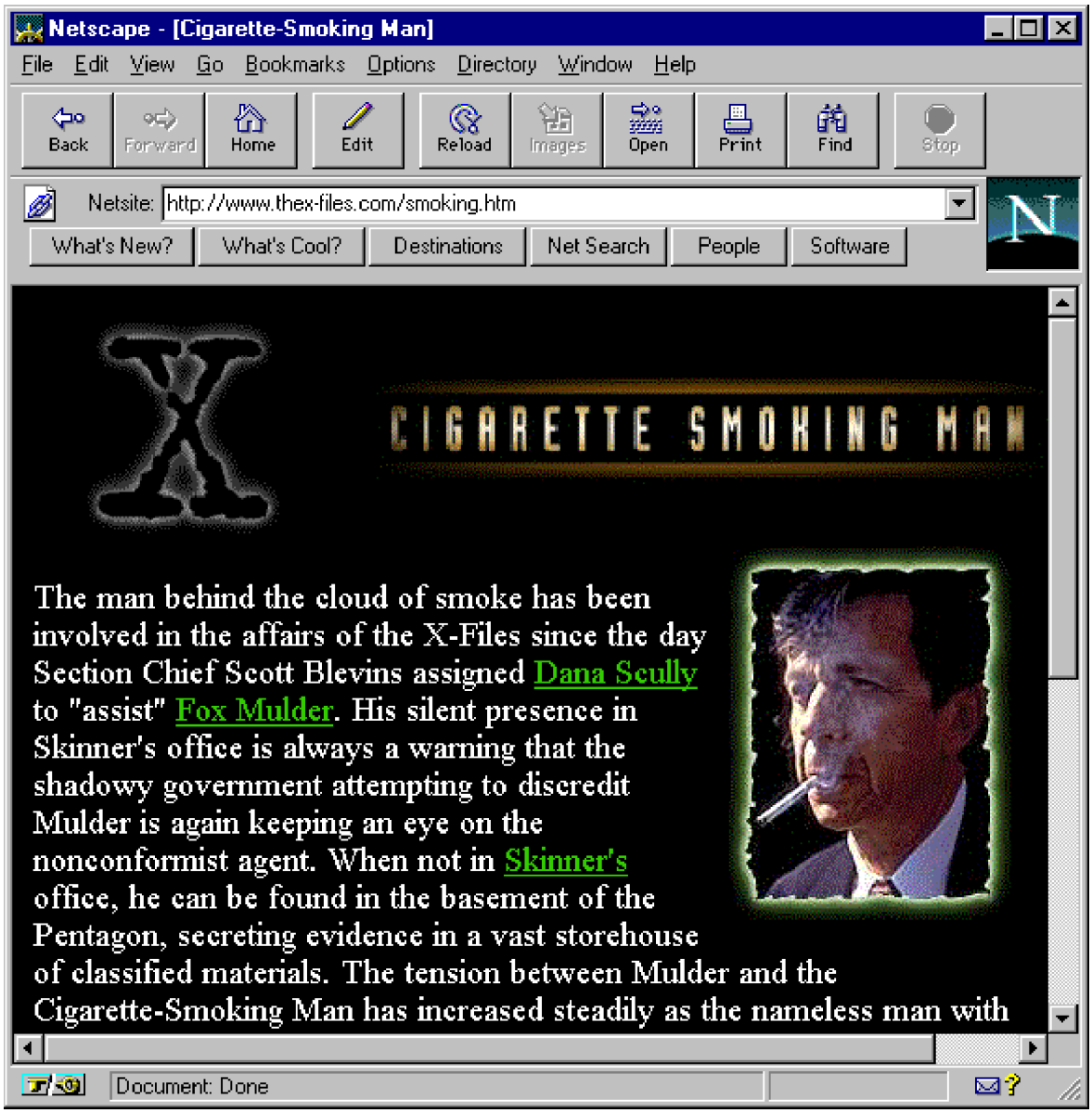
SECADD.EXE - oikeuksien lisääminen rekisteriin käyttäjille.

11. TIETOTURVALLISUUS

Turvallisuus on elintärkeää verkkoympäristössä. Käyttäjät tallentavat sijoittavat palvelimille muiden käyttäjien kanssa jaettavia tietoja ja organisaatiot käyttävät verkkoa operatiivisessa toiminnassaan. Niinpä järjestelmältä vaaditaan myös riittävää tietoturvaa.

Windows NT on yhä suositumpi käyttöjärjestelmä operatiivisissa järjestelmissä. Tässä luvussa käsitellään joitakin käytännön asioita, jotka täytyy ottaa huomioon tietoturvaa suunniteltaessa ja toteutettaessa, internet/intranetia unohtamatta. Pelkästään Windows NT tai mikään muukaan käyttöjärjestelmä ei poista turvaongelmia, koska mikään käyttöjärjestelmä ei pysty tarjoamaan täydellistä turvaratkaisua.

Niinpä *sinun* tulee määritellä omiin tarpeisiisi sopiva tietoturvan taso ja suunnitella Windows NT:n turvaominaisuuksien käyttö osaksi yleistä turvallisuusjärjestelmää. Turvajärjestelmään täytyy liittyä sekä fyysisiä että loogisia turvatoimenpiteitä ja sen ensisijaisena tavoitteena on rakentaa mahdollisimman hyvä vastustuskyky tunkeilijoiden ja onnettomuuksien varalta. Siksi seuraavat ohjeet menevät tiukimman mukaan. Sovella niitä parhaiten katsomallasi tavalla. Kuten Andy Groven kirjan nimi sanoo, *Only the Paranoid Survive*.



It s jungle out there! - Trust No 1

Tietoturvallisuuden suunnittelu ja toteuttaminen

Ennenkuin siirrymme Windows NT:n mahdollisuuksien tarkasteluun, on syytä unohtaa tekniset lähtökohdat rajoituksineen ja lähteä liikkeelle *tarpeista*. Koska tyypillisesti järjestelmän heikoin lenkki piilee **inhimillisessä tekijässä**, yksinkertaisin tietoturvan tehostaminen saavutetaan helposti johdonmukaisten toimintatapojen ja ohjeiden noudattamisella.

Ohjeistetut toimintatavat täytyy ottaa käyttöön koko organisaatiossa ja jokaisen täytyy ottaa vastuu niiden noudattamisesta.

Suuremmissa organisaatioissa voidaan palkata erityinen turvapäällikkö tai perustaa tietoturvatyöryhmä paikallistamaan tietoturvan puutteita, kehittämään toimintatapoja ja ottamaan niitä käyttöön. Tietoturvaa edistää myös tarkkaan määritelty eri tukihenkilöiden roolit selkeine vastuujakoineen ja selvästi määriteltyine käytäntöineen, esimerkiksi kuinka käyttäjätunnuksia luodaan ja kuinka käyttäjäoikeuksia eri resursseihin myönnetään.

Suunnittelun lähtökohdat

Kun järjestelmän tietoturvaa suunnitellaan, ensin täytyy määrittää nyt olemassa oleviin järjestelmiin liittyvät ongelmat ja muodostaa jonkinlainen kuva tavoitteista. Jos selkeää kuvaa tavoitteista ei ole, tietoturvan edellyttämä suunnitelmallisuus kärsii.

Kannattaa selvittää tämänhetkisestä tilanteesta esimerkiksi seuraavia asioita:

- Mitä ongelmia nykytilanteessa on - haastattele tukihenkilöitä, käyttäjiä, esimiestehtävissä toimivia - yleensä kaikkia ihmisiä, joilla on jotain tietoa ja turvallisuusongelmista ja -vaatimuksista

- Henkilöstöosastolta, jaospäälliköiltä ja osastopäälliköiltä pitäisi saada vuokaavioita, henkilöstöprofiileja, työnkuvauksia ja muita tietoja ihmisistä, datasta ja resursseista ja siitä, kuinka niitä hallitaan

- Määritä työnkuvausten pohjalta, millaisia käyttöoikeuksia eri käyttäjät tarvitsevat ja myönnä käyttäjille **aina** alin mahdollinen käyttöoikeustaso, jolla he tulevat toimeen tehtäviensä hoitamisessa

- Millaista suojausta tarvitaan? Tutustu fyysisten turvallisuusvaatimusten lisäksi järjestelmien ja sovellusohjelmien turvallisuusvaatimuksiin

- Arvioi jokaista osatekijää erikseen ja määritä sen tärkeys. Näin saat selville, mitkä järjestelmän osat vaativat kaikkein pikaisinta huomiota

- Selvitä järjestelmän kustannukset ja hanki sille rahoitus. Älä käytä liikaa rahaa sellaisiin turvajärjestelmiin, jotka ovat niin monimutkaisia, että käyttäjät jättävät ne käyttämättä

- Ota huomioon vastuukysymykset. Jos työntekijä- tai asiakastietoja joutuu vääriin käsiin, voit päätyä oikeuteen. Monikansallisissa organisaatioissa kannattaa huomioida aivan erikseen Yhdysvallat, jossa asuu 6 prosenttia maailman väestöstä, mutta 70 prosenttia maailman lakimiehistä

Jokainen näistä kohdista vaatii jonkun tietoturvaryhmän jäsenen erityisen huomion tai osaston, työryhmän tai osastopäällikön huomion organisaation koosta riippuen. Tietoturvaohjeita ja -suunnitelmia kehitettäessä täytyy kiinnittää huomiota ainakin seuraaviin (ehkä hieman diktatorisilta tai pessimistisiltä tuntuviin) asioihin:

- Fyysisiin turvatoimiin, joiden avulla voidaan estää varkauksia ja tarvittaessa varautua luonnonmullistuksiin

- Käyttäjien tietokoneiden turvaukseen, jolla estetään laitteiden ja tiedon varastaminen

- Salasanaohjeisiin, joiden avulla määritetään pitkiä, vaikeasti arvattavia (*mutta helposti muistettavia*) salasanoja tai koodausjärjestelmiin, jotka luovat vaikeasti arvattavia salasanoja fraaseista ja muita tiedoista

- LAN- ja WAN-verkkojen yhteyksien turvaamiseen, jotta voidaan estää luvaton linjojen tarkkailu ja käyttö

- Virusten ja Troijan hevosten etsimiseen koko verkosta

- Internet-tietoturvaan palomuureihin, WWW-palvelimen käytön valvontaan ja turvattuihin transaktioihin

- Sähköpostin valvontaohjelmiin (myös automaattinen virusskannaus) sekä sähköisten allekirjoitusten käyttöön viestien alkuperän varmistamiseksi

- Salausmenetelmiin, joiden avulla suojellaan tallennettuja tiedostoja, varmuuskopioita, sähköpostia ja tiedonsiirtoa yksityisissä tai julkisissa verkoissa

- Salausmenetelmiin, joiden avulla suojellaan kannettavilla tietokoneilla ja muilla henkilökohtaisilla tietokoneilla olevia tärkeitä tietoja

- Hallintarakenteisiin, joissa määritellään tukihenkilöt, pääkäyttäjät, paikalliset vastuuhenkilöt, käyttäjät, **tietoturvasta vastaavat henkilöt** (*Information security officer*) ja **tietoturvaohjeiden noudattamista valvovat henkilöt** (*Information security auditors*)

- Aktiiviseen valvontaan, jonka tavoitteena on havaita murtautumiset, hakkerointi (*krakkerointi*) ja työntekijöiden luvaton resurssien käyttö, apuna lokien määrittely ja jatkuva seuranta

- Tiedonsuojaussuunnitelmiin, jonka osana määritetään varmuuskopiointikäytäntö, varmuuskopioiden säilyttäminen muualla kuin yrityksen tiloissa ja menettelyt, joiden mukaan tietoja palautetaan varmuuskopioilta

- Menetelmiin sovellusohjelmien ja tiedon turvalliseen jakamiseen organisaation sisällä, myös eritasoisten tietoturvaohjeiden jakaminen

- Tunkeutumisien havainnointi- tai raportointitoimintatapoihin, joilla yritystä ja sen työntekijöitä suojellaan syytöksiltä väärinkäytöistä ja varkauksista

- Työntekijöiden koulutusohjelmiin, joiden tavoitteena on vähentää tietoturvariskejä ja määrittää toimintatavat ja oikeudelliset vastuukysymykset. Tämä tulisi toteuttaa osana uuden työnteki-

jän perehdytyskoulutusta ja toistaa säännöllisin väliajoin tai ainakin menetelmien muuttuessa.

Uudet valvontamenetelmät täytyy ottaa käyttöön koko organisaatiossa ja niitä täytyy noudattaa kaikilla alueilla. Epäonnistuminen yhdellä alueella luo tietoturva-aukkoja, jotka vaarantavat koko järjestelmän. Tavoitteena on kuitenkin löytää ja määrittää kaikki organisaatiota uhkaavat tietoturvaongelmat. Niinpä järjestelmää ja toimintatapoja täytyy arvioida jatkuvasti uudelleen, jotta havaittaisiin ajoissa organisaation tietoturvan vaarantavat uudet ongelmat ja aukot.

Toteuta laadittua suunitelmaa sopivalla vauhdilla. Monia uusia valvontamenettelyjä sisältävään järjestelmään täytyy siirtyä asteittain. Aloita vaiheittain ja tiukenna valvontaa vähitellen. Kannattaa muistaa lähtökohtana kaiken toiminnan loogisuus ja käyttäjien motivointi! Jos normaalien työtehtävien hoito kärsii tai vaikeutuu monimutkaisten ja huonosti toteutettujen menetelmien vuoksi, seuraa jälleen tietoturvan löystymistä. Yksinkertaiset, selkeät rutiinit ovat usein parempia kuin monimutkaiset tekniset apuvälineet.

Tiedonhallinta ja valvonta

Organisaatio omistaa tietenkin tuottamansa tiedot, mutta kuka valvoo näitä tietoja ja niiden käyttöoikeuksia?

Missä tietoja säilytetään?

Kuka hoitaa varmuuskopioinnin ja arkistoinnin?

Jos kattavaa **DataWarehouse-ratkaisua** ei ole tehty (ja vaikka olisikin), tavallisesti eri osastot, työryhmät tai jaokset pitävät itsellään luomiensa tietojen omistusoikeuden. Siksi on vaikeaa toteuttaa koko yrityksen kattavaa tietoturvasuunnitelmaa ja -menettelytapoja. Ryhmien kanssa täytyy olla läheisessä yhteistyössä, mutta jos mukana on liian paljon ihmisiä, seurauksena voi olla - ja yleensä onkin - kaaos. Ylemmän johdon täytyy ehkä antaa ohjeet keskitetystä tietoturvasuunnittelusta, jotta yrityksen tietoturvallisuus tulisi varmistettua. Tiedon omistajille täytyy selvittää heidän roolinsa ja vastuunsa tiedon turvaamisen suhteen.

Nämä asiat tulevat helposti asiakas-palvelinympäristöissä (*Client/Server*) monimutkaisiksi. Koska käyttäjillä on tehokkaat mikrotietokoneet, he voivat tallentaa paikallisille levyasemille tallennettavia tietoja. Voidaanko

nämä tiedot suojata hakkereilta, varkailta ja vahingoittumiselta?

Ympäri verkkoa olevan tiedon hallitseminen voi olla painajaismaista, mutta myös tiedon keskittäminen tietokeskukseen voi olla lähes mahdoton tehtävä. Se luo uusia vaatimuksia kuten tarpeen suojautua paikallisilta katastrofeilta tai parantaa verkon vastausaikaa verkon lisääntyneen käytön vuoksi. Lisäksi standardit, protkollat, sovellusohjelmat ja tiedostoformaatit tuovat omia ongelmiaan. Eräs syy internet-protokollien ja -tekniikoiden suosion kasvussa onkin ollut mahdollisimman laajan yhteisen nimittäjän etsiminen (esimerkiksi FTP- ja HTTP-protokollat, HTML-kuvauskieli).

Keskitettyyn toimintaan liittyy tietenkin myös etuja: palvelimia ja muita laitteita voidaan säilyttää turvallisissa huoneissa, joissa koulutettu henkilökunta huolehtii järjestelmistä ja valvonnasta. Keskitetyssä ympäristössä varmuuskopiointijärjestelmät ovat myös helpompia toteuttaa kuin täysin hajautetussa ja useimmiten kustannuksetkin ovat alhaisemmat.

Käyttöoikeudet

Kuka ja millä perusteilla päättää, kenellä on oikeus käyttää tietoja ja millä tasolla? Tämä prosessi käy helpommaksi, jos käyttäjistä muodostetaan ryhmiä *tilapäiset työntekijät*, *toimistotyöntekijät*, *osastopäälliköt* ja niin edelleen. Työryhmät muodostuvat samassa projektissa tai saman prosessin parissa työskentelevistä ihmisistä, ja niiden jäsenet eivät välttämättä edes työskentele samalla osastolla.

Esimerkiksi uuden tuotteen suunnittelutyöryhmässä voi olla jäseniä kehitys- tai suunnitteluosastolta, markkinointiosastolta, myyntiosastolta ja hallinnosta. Eri ryhmien käyttöoikeudet voi määrittää tietoturvaohjeita suunnittelevista esimiehistä koostuva ryhmä. Asiat eivät ole mallillaan, jos tukihenkilöt määrittelevät uusia käyttäjiä luodessaan samalla käyttäjien ryhmäjäsenyydet, oikeudet ja käytettävissä olevat resurssit.

Koska Windows NT:n käyttäjäryhmät ja käyttöoikeustasot koostuvat useista eri hallinto- ja käyttäjätasoista, voit luoda hierarkkisen rakenteen, joka määrittää seuraavien ryhmien käyttöoikeudet:

- **Ylimmän tason pääkäyttäjä tai tukihenkilö** - henkilö, joka hallitsee Window NT -palvelimen **Administrator**-käyttäjätunnusta, jäsenyys päätoimialueen (*Master Domain*) paikallisessa

Administrators-ryhmässä sekä **Domain Admins-ryhmässä** (ks. myös **toimialuemallien** kuvaus Luvusta 6). Käyttäjätunnus voi olla jokin muukin, mutta siitä tulisi olla kopio. Molempien käyttäjätunnusten salasana tulisi olla suljetussa kirjekuoressa lukitussa esim. paloturvakaapissa rajoitetusti ja valvotusti saatavilla

- **Paikalliset pääkäyttäjät tai muut tukihenkilöt** - eri osastojen, työryhmien ja jaosten tukihenkilöt, jotka valvovat ja hallitsevat paikallisia verkkoja ja tietoresursseja. Nämä voivat käyttää luottavan toimialueen paikallista **Administrator**-käyttäjätunnusta, olla jäsenenä kyseisen toimialueen paikallisessa **Administrators-ryhmässä** sekä kyseisen toimialueen **Domain Admins-ryhmässä** (ks. myös **toimialuemallien** kuvaus Luvusta 6). Käyttäjätunnuksen olisi syytä olla tukihenkilökohtainen, esimerkiksi **ADMIN_JKI**. Toimialueen **Administrator**-käyttäjätunnuksesta tulisi olla kopio ja näiden salasanat tulisi olla vain rajoitetusti ja valvotusti saatavilla

- **Luottokäyttäjät** - työntekijät, joilla on pääsy luottamuksellisiin tietoihin. Esimerkiksi päätoimialueen (*Master Domain*) **Domain Users-ryhmän** jäsenet - ryhmä on mukana luottavan toimialueen paikallisessa **Users**-ryhmässä

- **Tilapäistyöntekijät** - uusia käyttäjiä tai käyttäjiä, joiden työnkuva on tarkkaan rajattu - esimerkiksi kesäharjoittelijat, määräaikaiset työntekijät, ja vaikkapa konsultit. Käyttäjät ovat mukana esimerkiksi vain paikallisessa **Users**-ryhmässä

- **Riskikäyttäjät** - työntekijät, joiden pääsyä verkkoresursseihin on erityisesti rajoitettu

- **Yleiset käyttäjät** (*Public Users*) - jos organisaatio on yhteydessä internetiin, internetin käyttäjillä voi olla rajattu oikeus käyttää tiettyjen palvelimien tietoja. Tässä tapauksessa näiden käyttäjien käyttöoikeudet on yleensä rajattu tarkkaan ja vain tiettyihin palvelimiin. Järjestelmän käyttöoikeuteen voidaan vaatia salasana, jolloin saadaan selville, kuka järjestelmää käyttää

- **Anonyymikäyttäjät** (*Anonymous Users*) ja vierailijat (*Guests*) - yleisiä käyttäjiä tai sisäisiä käyttäjiä, jotka kirjautuvat verkkoon ja saavat käyttöönsä resursseja ilman käyttäjätunnusta ja sa-

lasanaa. He voivat käyttää tarkkaan rajattuja resursseja yleisillä anonyymi- tai vierailijakäyttäjätunnuksilla. Kyseessä voisi olla vaikkapa paikallisen **Guests**-ryhmän jäsenet

Ne, jotka eivät kuulu mihinkään edellämainituista ryhmistä, ovat todennäköisesti **tunkeutujia**. Sellaiseksi voidaan katsoa kuka tahansa käyttäjä, jolla ei ole käyttöoikeutta verkon mihinkään resurssiin. Tämä kattaakin kaikki ne käyttäjät, jotka syystä tai toisesta pääsevät käyttämään verkon resursseja ilman käyttöoikeuksia tai vaadittua auktorisointia.

Pääkäyttäjät tai verkkovastuuhenkilöt

Windows NT -palvelimen tai verkon pääkäyttäjällä on suunnaton määrä valtaa. Hän hallitsee järjestelmän kaikkia resursseja ja tietoja, ja pääsee tarvittaessa kaikkiin resursseihin käsiksi. Vastuuhenkilön tehtävä ei ole mikään mitätön *toisen käden* tai *o.t.o.* tehtävä, vaan täysipäiväinen toimi, jota hoitamaan tarvitaan pätevä henkilö.

Turvallisuussyistä saattaa olla myös syytä selvittää tehtävään valittavan henkilön tausta.

Joissakin organisaatioissa eri henkilöiden muodostama ryhmä voi hoitaa kaikkein korkeimman tason hallintatehtävät. Tällöin jokaisella ryhmän jäsenellä on silloin hallussaan osa salasanasta, ja osat täytyy antaa yhdessä toisten jäsenten osien kanssa, jotta järjestelmää voidaan käyttää.

Windows NT -ympäristö muodostuu **toimialueista** (*domain*). Ne ovat eri osastoihin, divisiooniin, työryhmiin tai muihin rakenteisiin kuuluvien NT-palvelimien ja käyttäjien työasemien muodostamia ryhmiä, joiden sisällä hallinnoidaan keskitetysti eri käyttäjätunnukset ja -ryhmät oikeuksineen. Eri toimialueiden välillä voi olla luottosuhde, jolloin yhden toimialueen käyttäjä voi käyttää myös muiden toimialueiden resursseja. Kullakin toimialueella voi olla oma pääkäyttäjänsä, joka joko määrittää toimintatavat tai on vastuussa ylemmän tason pääkäyttäjälle, joka määrittää koko organisaation toimintatavat.

Toimialueiden pääkäyttäjät päättävät, kuinka eri toimialueiden väliset luottosuhteet määritetään. Tässä mallissa on kuitenkin joitakin mahdollisuuksia tietoturvaongelmien syntymiselle. Jos pääkäyttäjät saavat vapaasti myöntää käyttöoikeuksia eri toimialueiden välillä, voi helposti syntyä tietoturva-aukkoja. Tietoturvaa voidaan parantaa, jos koko yrityk-

sen pääkäyttäjä tarkistaa ja määrittää toimialueiden väliset luottosuhteet. Tällöin kyseessä on tavallisesti päätoimialueen (*Master Domain*) **ylimmän tason pääkäyttäjä tai tukihenkilö**.

Suurissa organisaatioissa on apulaispääkäyttäjiä, jotka hallitsevat joko verkon eri resursseja tai haarakonttoreiden järjestelmiä. Nämä pääkäyttäjät eivät välttämättä aina tunne tarkkaan hallitsemansa järjestelmän toimintaa ja voivat siksi tarvita yksityiskohtaisia ohjeita voidakseen hoitaa tehtäväänsä paremmin. Kaikki järjestelmän pääkäyttäjät tulee kouluttaa tehtäväänsä hyvin.

Jos organisaatiossa on käytössä useita eri järjestelmiä, turvaohjeita on vaikea toteuttaa käytännössä, koska keskustietokoneissa ja verkkopalvelimissa on erilaiset turvajärjestelmät. Pääkäyttäjien ryhmässä tulee silloin olla henkilöitä, jotka tuntevat eri järjestelmien turvallisuus- ja hallintavaatimukset.

Tietoturvasta vastaava henkilö (*Information security officer*) on organisaation tietoturvamenettelyjen suunnitteluun, toimeenpanoon ja valvomiseen erikoistunut henkilö. Hänellä täytyy olla tekninen tausta, jotta hän pystyy päihittämään ovelat hakkerit ja hyökkääjät, ja hänen tulee tuntea tarkkaan käyttöjärjestelmän, verkkoyhteyksien, verkon valvontalaitteiden (snifferit, nuuskijat) ja analyysivälineiden toiminta sekä eri menetelmät ongelmien havaitsemiseksi ja tunkeutujien kiinnisaamiseksi. Hänellä tulisi olla hyvä business-vaisto (voidakseen arvioida akuutit tietoturvaongelmat ja mahdolliset hyökkäyksen kohteet) ja taito työskennellä organisaation muiden jäsenten kanssa. Nämä henkilöt ovat itse asiassa turvallisuuspoliiseja, jotka etsivät ja jäljittävät mahdollisia tietoturvaongelmia. Heidän tehtävänään on varmistaa yhtäläinen tietoturvataso koko organisaatiossa, jotta heikkoja kohtia ei jäisi. Eräs tehtävä on kerätä työntekijöiltä tietoja turvallisuusrikkomuksista ja epäilyttävistä yhteydenotoista. Jo pelkästään aktiivisen tietoturvasta vastaava henkilön olemassaolo parantaa tietoturvallisuutta, koska se tarkoittaa sitä, että joku henkilö keskittyy pelkästään organisaation turvallisuusasioihin.

Suurissa organisaatioissa käytetään erillisiä valvojia, **tietoturvaohjeiden noudattamista valvovia henkilöitä** (*Information security auditors*) joiden tehtävänä on tunnistaa epäilyttävää toimintaa, lipsumisia suositelluista menettelytavoista ja muita tietoturvaongelmia. Valvoja tarkkailee kaikkien työntekijöiden toimintaa, myös pääkäyttäjien ja vastaavien. Valvojan täytyy toimia jollakin tavoin erillään muusta organisaatiosta.

Verkon hallintavastuu

- Verkkoonpääsyn valvonta:
  - Kuka määrittelee ja miten käyttäjätunnukset, salasanat ja käyttöoikeudet, työasema- ja aikarajoitukset, etäyhteydet...
- Verkon toiminnan seuranta:
  - Kuormitus, lokit, muutokset, hälytykset...
- Ohjelmisto- ja laiteasennukset:
  - Millaisia laitteita ja ohjelmia
  - Kuka hankkii, asentaa ja ylläpitää
  - Ohjelmisto- ja hankintapolitiikka
- Tehtäviä:
  - Kuuntele käyttäjiä ja opasta käyttäjiä
  - Seuraa tilannetta, ongelmalokikirja
  - En tiedä - otan selvää
  - Pysy ajan tasalla, testaa
  - Ylläpitosuunnitelma, standardit ja rutiinit (uudet käyttäjät, koulutus)
  - Toipumissuunnitelma, varmistukset, varalaitteet
  - Dokumentointi ja ohjeistus

Käyttäjien koulutus

Koulutuksen avulla voidaan varmistaa, että käyttäjät ottavat turvallisuusohjeet tosissaan. Suurissa organisaatioissa on elintärkeää, että jokainen organisaation jäsen noudattaa turvallisuusohjeita johdonmukaisesti.

Jos käyttäjät eivät ole tietoisia turvallisuusriskeistä ja turvaohjeista, tuloksena on puutteita turvallisuudessa, onnettomuuksia, tiedon menetyksiä ja muita ongelmia. Voit parantaa luottamusta verkon turvallisuuteen kouluttamalla käyttäjiä. Käyttäjille kannattaa opettaa seuraavia asioita:

- Organisaation turvallisuustoimintatavat
- Henkilö- ja yritystietojen luottamuksellisuus
- Organisaation tietojen salassapito
- Kirjautumistietojen salassapito.

Käyttäjien koulutuksen jälkeen kannattaa pyytää jokaista allekirjoittamaan lausunto, jossa he todistavat ymmärtävänsä ja hyväksyvänsä verkonkäytön toimintatavat ja ohjeet. Lausuntoa voidaan käyttää muistutuksena (tai ikävimmässä tilanteessa todisteena), jos työntekijä saadaan kiinni verkon tarkoituksellisesta väärinkäytöstä.

Kerro käyttäjille, mitkä käyttöoikeudet heillä on verkon resursseihin, jotta he eivät yritä päästä käyttämään tiedostoja tai laitteita, joita heillä ei ole lupaa käyttää. Voit myös kertoa, kuinka valvontajärjestelmä seuraa käyttäjien toimia!

Voit kouluttaa työntekijöitä koulutustapahtumissa, tiedotuslehtien (joko perinteisten painettujen, sähköpostissa, News- tai WWW-palvelimella levitettävien), esitteiden ja muiden menetelmien avulla. Voit jopa järjestää tietoturvaharjoituksia.

Käyttäjien koulutus

- Työaseman/mikron peruskäyttö:
  - Salasanat/ käyttäjätunnukset
  - Mikron perusteet
  - Käyttöliittymät, Windows ja valikot
  - Minimi verkko-osaaminen
  - Tiedostojen käsittely (tallentaminen, tiedostonimet, hakemistot, levyasemat)
  - Levykkeiden käsittely
  - Tietojen tuhoaminen ja salakirjoitus
  - Kirjoitinten ja tulosteiden käyttö
- Asennekoulutus:
  - Mikrojen kuljettelu työpaikan ulkopuolelle tai työpaikalle
  - Luvattomat ohjelmat ja luvattomat kopiot
  - Työasemien sulkeminen tai lukitseminen poistuttaessa työpaikalta
  - Mikron asiaton käyttö
- Ilmoitukset ongelmista

Katastrofista toipuminen

Olennainen osa tietoturvatoimintatapoja on toipuminen katastrofeista. Kuinka pitkälle liiketoiminnan jatkuminen riippuu tietojärjestelmistä? Voiko toiminta jatkua manuaalisesti, jos järjestelmät ovat käyttökelvottomia pitkiä aikoja?

Järjestelmän kaatuminen voi maksaa sadoista tuhansista miljooniin markkoihin ja mahdollisesti työpaikkasi, kunhan savu ensin hälvenee.

On syytä tunnistaa organisaation kriittiset sovellukset ja palvelut sekä tunnistaa sitten niiden vaatimat laitteistot ja muut riippuvuussuhteet järjestelmään. Seuraa myös mahdollisia muutoksia organisaation tärkeimmäksi katsotussa järjestelmässä.

Kannattaa pitää varalaitteita lähettyvillä tai rakentaa toinen tiedonhallintakeskus riippuen siitä, kuinka paljon rahaa on käytettävissä ja kuinka tärkeää tieto on. Varalaitteet voivat olla siunaus katastrofin sattuessa. Ne vanhat PC:t, jotka hylättiin siirryttäessä parempiin järjestelmiin, voidaan varastoida johonkin muualle kuin päätoimipaikkaan. Varastotilaan voidaan rakentaa pieni palvelinverkko, jota voidaan tarvittaessa helposti laajentaa. Hätätilanteessa joitakin kiireellisiä tehtäviä voidaan ehkä tarvittaessa hoitaa tällä verkolla.

Tärkein toipumisväline ovat **varmuuskopiot**. Testaa varmuuskopiot ja menetelmät, joiden avulla tiedot voidaan palauttaa. Säilytä varmuuskopioita pysyvinä arkistoina jossain muualla kuin yrityksen tiloissa. Joudut ehkä käymään läpi useita varmuuskopioita, jos joku on tarkoituksella tuhonnut tietoja tai virukset ovat pilanneet tietoja.

Pidä kirjaa järjestelmäasetuksiin, käyttäjiin ja datatiedostoihin tehdyistä muutoksista. Joudut todennäköisesti tekemään muutokset uudelleen tietojen palauttamisen jälkeen.

Monistuspalvelimet (*Replicator Server*) voivat antaa suojaa paikallisia katastrofeja vastaan kopioimalla tietoa reaaliaikaisesti muualla sijaitseviin palvelimille. Harkitse myös useiden yhteyksien luomista eri toimipaikkojen välille, jolloin yhden linkin katketessa toinen voi jatkaa toimintaa.

Parhaassa tapauksessa linkit kulkevat eri polkuja ja muodostavat yhteyden eri palveluntarjoajien kautta.
Muodosta hätätilanteiden varalta erityinen ryhmä ja kouluta sen jäsenet

käsittelemään ongelmia, jos niitä ilmenee esimerkiksi viruksia tai laitteistovikoja. Ryhmällä on oltava johtaja, joka toimii koordinaattorina, kun suunnitellaan toimia katastrofin varalta. Hän ohjaa hätätilanneharjoituksia ja varsinaisia hätätilanteita.

Suunnitelkaa:

- Välitön toiminta, kun ongelma havaitaan. Jos esimerkiksi palvelimelta löytyy virus, voidaan peruuttaa suunniteltu varmuuskopiointi tai estää tietojen monistaminen toisille palvelimille, lisäksi esimerkiksi sähköposti tai FTP/WWW-palvelin voidaan sulkea

- Yhteyden ottaminen henkilöihin, jotka rakentavat järjestelmät uudelleen, syöttävät uudelleen kadotetut kriittiset tiedot tai hoitavat luottamuksellisten tietojen palautuksen

- Vaiheet järjestelmien saattamiseksi takaisin käyttökuntoon tai toimintojen siirtämiseksi varatoimipaikkaan

- Halutunlainen järjestelmien uudelleenrakentaminen

- Varmuuskopioiden noutaminen niiden säilytyspaikasta ja tietojen palauttaminen.

Koska prosessissa on monia vaiheita, ja turvallisin lähestymistapa on kehittää hyvä suunnitelma, joka voidaan testata ja todistaa hätätilanteessa toimivaksi.

Tietoturvaohje

Tietoturvaohje on organisaation lausunto siitä, kuinka se huolehtii turvallisuudesta, käsittelee tunkeutumisia ja toipuu turvallisuusonnettomuuksien aiheuttamista vahingoista. Siinä määritetään työntekijöiden toimintaohjeet ja kuinka tietoturvaa hallitaan.

Tarvittaessa tietoturvaohje voidaan jopa sisällyttää työsopimuksiin ja pitää mukana jonkinasteinen **käyttäjän vastuu**, jotta voidaan varmistua siitä, että käyttäjät noudattavat ohjeita. Valvo ohjeiden noudattamista eri valvontamenetelmillä ja jäljitä käyttäjät, jotka voivat eivät toimi ohjeiden mukaan. Lähetä yrityksen uutisryhmiin ja kirjautumisilmoituksiin muistutuksia turvaohjeista.

Kun ohjeet on saatu valmiiksi, niiden noudattaminen on tärkeää, jotta koko organisaatiossa säilytetään sama turvallisuustaso. Tämä ei kuitenkaan tarkoita, että mitään vaihtelua ei sallittaisi. Itse asiassa ohjeen täytyy olla riittävän joustava, jotta se sallii muutokset ohjeissa. Muutokset täytyy kuitenkin käsitellä asianmukaisesti. Päällikköjen tai käyttäjien ei saa antaa tehdä muutoksia omin päin. Johdon täytyy hyväksyä kaikki muutokset ja ne täytyy kirjata ohjeen lisäykseksi.

Ohjeisiin kerätään suurten, vaikeaselkoisten asiakirjojen ja monimutkaisten, usein noudattamatta jätettävien sääntöjen **tärkeimmät** asiat. Pidä tavoitteena ohjetta, joka on erittäin helppo ottaa käyttöön ja jota käyttäjien helppo ymmärtää ja noudattaa.

Itse asiassa tietoturvaohjetta tärkeämpi on luultavasti ohjeen kehittämisprosessi, koska se pakottaa tarkastelemaan kaikkia niitä asioita, jotka tulee ottaa huomioon riittävän tietoturvatason takaamiseksi organisaatiolle. Mieti myös jo etukäteen, mitä teet, jos järjestelmään tunkeudutaan tai jokin katastrofi tapahtuu. Ohje on väline, jonka avulla voi valmistautua pahimpaan.

Turvastandardeja

Yhdysvaltojen kansallisen turvallisuuspalvelun **National Security Agencyn** (NSA) yksikkö **National Computer Security Center** (NCSC) on hahmotellut tietoturvavaatimuksia vuodesta 1967, ja viimeiset määritykset valmistuivat 1980-luvun puolivälissä. Dokumentit ovat julkisia asiakirjoja. Dokumentissa **Trusted Computer System Evaluation Criteria** (TCSEC, tietokonejärjestelmän arviointikriteerejä). TCSEC tunnetaan paremmin nimellä **Oranssi kirja** (Orange Book). Standardissa määritetään tietokonejärjestelmille käytönvalvontamenetelmiä, joita noudattamalla tietokonetoimittajat voivat noudattaa Yhdysvaltain puolustusministeriön (*Department of Defense*, DoD) turvallisuusohjeita. Oranssi kirja käsittelee yksittäisiä tietokoneita ja käyttöjärjestelmiä. Tietoverkkojen turvallisuusohjeita on määritetty **Punaisessa kirjassa** (Red Book) eli oppaassa **Trusted Network Interpretation**. **Laventelinsininen kirja** (Lavender Book) keskittyy tietokantoihin. Kirjoja on yli 20, ja niitä kutsutaan nimellä **Sateenkaarisarja** (Rainbow Series).

Suojausluokitukset ovat seuraavat:

D - minimisuojaukset (Minimal Protection)

C - toimintavapauksien rajoittamat suojaukset (Dicretionary Protection)

B - pakollinen suojaus (Mandatory Protection)

A - varmennettu suojaus (Verified Protection).

Luokitukset menevät järjestyksessä pienimmästä suurimpaan turvallisuuteen:

C1➡C2➡B1➡B2➡B3➡A1

C2-luokitus viittaa turvaohjeisiin, joissa määritetään turvallisen järjestelmän toimintaa. Edellytyksiä C2-luokituksen myöntämiselle ovat:

- Hyvä dokumentaatio sekä peruskäyttäjälle että pääkäyttäjälle ja dokumentaatio suojauksien testaamisesta
- Käyttäjien auktorisoiminen yksittäisinä käyttäjinä
- Objektien uudelleenkäyttämisen esäminen niiden poistamisen jälkeen
- Pääkäyttäjien mahdollisuus tarkastaa kaikkia suojaustapahtumia sekä yksittäisten käyttäjien toimintaa
- Suojata kaikki objektit ja prosessit toisiltaan.

National Security Agency myönsi elokuussa 1995 Window NT Server- ja Workstationille (versio 3.5) **C2-turvallisuusluokituksen**. Tästä syystä Windows NT on NSA:n EPL-listalla (*Evaluated Programs List*, arvioitujen tuotteiden luettelo). EPL-listalla oleminen tarkoittaa, että Windows NT -käyttöjärjestelmän avulla voidaan saavuttaa C2-turvallisuusluokitus omassa järjestelmässä.

Tässä kohdassa on syytä tehdä eräs tarkennus. **Käyttöjärjestelmä** ei sinällään saa koskaan C2-luokitusta. Sertifiointi pätee vain täydelliseen kokoonpanoon, joka sisältää käyttöjärjestelmän lisäksi laitteiston, ohjelmat ja ympäristön, johon järjestelmä asennetaan. Sertifiointi koskee

lisäksi tiettyä versiota. Niinpä vaikka NT 3.5 Service Pack 3:lla onkin saanut C2-sertifikaatin, mikä tahansa lisäys tai korjaus purkaa sertifikaatin - esimerkiksi Service Pack 4:n asennus.

C2:ssa määritetty turvamenettely on nimeltään **Discretionary Access Control** (DAC). Windows NT:ssä se toteutetaan järjestelmänä, jossa käyttäjät omistavat (*Ownership*) objekteja. Tiedostojen kaltaisia objekteja on helppo ymmärtää, Leikepöytä (Clipboard) ja ikkunat ovat jo hieman hankalampia. Käyttäjät valvovat omistamiensa objektien käyttöoikeuksia ja ovat vastuussa kaikista objektin käyttöoikeuksiin liittyvistä toiminnoista.

Järjestelmä eroaa NSA:n **B-tason** turvallisuudesta, jossa määritellään luokitellut objektit ja **Mandatory Access Control** (MAC) -järjestelmä. Siinä objektien turvallisuustaso määritetään omistajasta riippumatta. Jos käyttäjä vastaanottaa salaiseksi (*Secret*) merkityn tiedoston, hän ei voi antaa muille käyttäjille oikeuksia katsella tiedostoa, jos näillä käyttäjillä ei myös ole Secret -turvaluokitusta. B-tasoa saatetaan myös käyttää suojattaessa pankkien, vakuutusyhtiöiden jne järjestelmiä.

Turvallisuusluokituksien arvostelijat ovat (aivan oikein) esittäneet, että Yhdysvaltain puolustusministeriön turvallisuusvaatimukset eivät kuitenkaan päde enää nykyisissä laajoissa yhtymätason tietojenkäsittelyjärjestelmissä. Onkin hyvä huomata, että C2-turvallisuusluokitus ei puutu mitenkään seuraaviin asioihin:

- Käyttöoikeuskomponettien jakelu ja luoton valtuutus
- Avainten hallinta ja sähköiset allekirjoitukset (*Digital Signature*)
- Salakirjoitusmenetelmät ja -protokollat
- Hajautetun sovellusympäristön suojaukset
- Verkon suojausvaatimukset, lähiverkon (LAN) ja laajan verkon (WAN) suojaukset
- Relaatiotietokantojen suojaukset ja muut tietokantoihin liittyvät suojaukset.

Tietoja käyttöjärjestelmien turvallisuussertifikaattien vaatimuksista löytyy **National Computer Security Conferencesta** (NCSC),

http://www.radium.ncsc.mil/.

Microsoft ja Novell keskustelevat siitä, kummalla on parempi C2-toteutus - ks. **http://www.microsoft.com/ntserver/c2bltn.htm**.

Lisätietoa tietoturvallisuudesta

On olemassa useita organisaatioita ja yrityksiä, jotka auttavat tietoturva- ja tietojärjestelmien rakentamisessa, turvatarkastuksissa, analysoivat tietoturvan heikoimpia kohtia, kehittävät ja arvioivat tietoturvaohjeita ja suunnittelevat ja toteuttavat tietoturvajärjestelyjä organisaatioille. Lisäksi tietoturvatuotteita on saatavissa eri käyttötarpeisiin.

Tällaisia ovat esimerkiksi:

- **Teleware Oy**, **http://www.teleware.fi**
- **Data Fellows Oy, http://www.datafellows.fi**
- **Nixu Oy**, **http://www.nixu.fi**
- **Narda Oy** on erikoistunut Windows NT-tietoturvaan, **http://www.narda.fi**.
- **NetEgrity** (*Leading Provider of Security Solutions*) konsultoi organisaatioita tunnistamaan ja estämään tietoturvariskejä, jotka liittyvät internetin ja intranettien käyttöön liiketoiminnassa. Lisätietoja: **http://www.security.com**.
- **CERT** (Computer Emergency Response Team) seuraa internetiin liittyviä tietoturvaongelmia. Se antaa neuvoja, turvavihjeitä ja tietoa järjestelmiin tunkeutumisen estämiseksi ja tapahtuneesta tunkeutumisesta selviämiseen. Lisätietoja CERT:in sivuilta **http://www.cert.org**
- **Computer Security Institute** (CSI) on kansainvälinen organisaatio, joka kouluttaa tietoturva-asiantuntijoita ja tarjoaa runsaasti tietoja sekä jäsenille että muille kiinnostuneille. Se julkaisee useita tiedotuslehtiä ja järjestää konferensseja ja näyttelyitä. Lisätietoja: **http://www.gocsi.com**

- **Information System Security Association** (ISSA) on kansainvälinen tietoturva-ammattilaisten organisaatio, joka tuottaa koulutusmateriaalia, julkaisuja ja yleistä tietoutta tietoturvaan liittyvistä asioista. ISSA:n tavoitteena on edistää hallinnollisia käytäntöjä, jotka varmistavat tietokoneilla ja verkoissa olevien resurssien käytettävyyden, koskemattomuuden ja luottamuksellisuuden. Lisätietoja: **http://www.uhsa.edu/issa/index.html**

- **Infosecurity News** tarjoaa työkaluja, menetelmiä ja tuotetietoutta. Lisätietoja: **http://athens.bitwise.net/isn/news.htm**

- **National Computer Security Association** tarjoaa tietoja ja materiaalia tietoturvasta yleensä. Lisätietoja: **http://www.ncsa.com**.

Muita Internet-osoitteita tietoturvasta ja Windows NT:stä:

- **The Royal Institute of Technology**, **http://www.it.kth.se/~rom/ntsec.html**

- **C2 Evaluation**, **http://www.microsoft.com/NTServer**

- **National Computer Security Center**, **http://www.radium.ncsc.mil/tpep/epl/index.html**

- **RSA-suojausmenetelmä-FAQ**, **http://www.rsa.com/rsalabs/newfaq**

- **Secure Socket Layer-FAQ**, **http://www.consensus.com/security/ssl-talk-faq.html**

- **SSH** jne, **http://www.cs.hut.fi/ssh/crypto**

- **U.S. Armyn** salauskäsikirja, **ftp://hubert.wustl.edu/pub/armycryp.zip**

- **U.S. DOE Computer Incident Advisory Capability**, CIAC, **http://ciac.llnl.gov**

- **Incident Response Teams**, FIRST, **http://www.first.org/**

- **Telstra**, **http://www.telstra.com.au/info/security.html**

- **COAST**, **http://www.cs.purdue.edu/coast/coast.html**
- **SomarSoft, http://www.somarsoft.com**
- **http://www.omna.com/yes/mwc/security.htm**
- **Bill Stout**, **http://www.hidata.com** (tarvitsee salasanan ja tunnuksen)
- **The NT Shop, http://www.ntshop.com/**
- **Internet Security Systems, http://www.iss.net**
- **Microsoft, http://www.microsoft.com/security**.

Suojauksiin liittyviä bugeja jne:

- **Windows NT Magazine**, **http://www.winntmag.com**
- **http://www.ntinternals.com**
- **BugNet**, **http://www.bugnet.com**
- **http://www.NTSecurity.com**.

Vaikka internetistä löytyykin todellistä tietoa, löytyy myös tietoa NT:n suojausmenetelmistä ja -ongelmista. NT:n tuntemus auttaa asettamaan internetissä roihuavat NT Security Flaw -keskustelut oikeaan kategoriaan. Kuten muissakin suojausongelmissa, tärkeintä on **maltti** sekä **todellisten ongelmien suuruusluokan arviointi** ja asian **tutkiminen** sopivilla menetelmillä.

Tom Sheldon on tunnettu Windows NT -tietoturva-asiantuntija, jonka julkaisee tietoja Windows NT -verkoista ja Windows NT:n tietoturvasta, myös koulutustapahtumista ja videokoulutusmateriaaleista. Lähettämällä nimesi ja osoitteesi pääset yksityiselle postituslistalle:

Windows NT Security Update Notes
P. O. Box 947
Cambria, CA 93428
USA

Kirjoja:

- **Windows NT Security Handbook** (Tom Sheldon), Osborne McGraw-Hill
- **Internet-tietoturva** (Nikander ym.), Suomen ATK-Kustannus Oy
- **Intranet and Internet Firewall Strategies** (Amoroso, Sharp), PC Week
- **Guide to Security and Data Integrity** (Farley ym.), LAN Times
- **Applied Cryptography** (Schneier), John Wiley & Sons
- **Computer Security Basics** (Russell ym.), O´Reilly & Associates
- **Practical UNIX & Internet Security** (Garfinkel, Spafford), O´Reilly & Associates
- **PGP: Pretty Good Privacy** (Garfinkel), O´Reilly & Associates
- **Windows NT Security Guide** (Sutton), Addison-Wesley Developers Press
- **Computer Hacking - Detection and Protection** (Malik), Sigma.

Lisäksi voisi mainita CSI:n oppaan **Manager s Guide to Computer Security Awareness**. Siinä kerrotaan, kuinka voidaan käynnistää tietoturvaohjelma ja kuinka käyttää eri menetelmiä tiedon levittämiseen tietokoneiden käyttäjille. Lisätietoja: **http://www.gocsi.com**.

Windows NT:n suojausjärjestelmä

Windows NT:tä ei voi asentaa ilman sen monipuolisia turvaominaisuuksia. Jos asentaminen ilman turvaominaisuuksia olisi ylipäätään mahdollista, lopputuloksena järjestelmä muistuttaisi enemmän Windows 95:ttä kuin Windows NT:tä.

Asennuksen aikana tehtäviä oletusasetuksia ei kuitenkaan välttämättä ole aina ajateltu ensisijaisesti tiukan tietoturvan kannalta, vaan asetuksia täytyy arvioida ja päivittää tarpeiden mukaan. Ohjeita ja vinkkejä annetaan myöhemmin tässä luvussa.

Windows NT:n turvallisuusominaisuuksia leimaakin se, että ne on upotettu varsin syvälle käyttöjärjestelmään. Vaikka Windows NT:n turvallisuusominaisuudet voivatkin näyttää monimutkaisilta, niillä saavutetaan kaksi yksinkertaista tavoitetta:

- **Pääsyn rajoittaminen** esimerkiksi järjestelmän resursseihin, tiedostoihin ja laitteisiin

- **Valvontapalvelut** (*Audit*), jotka luovat lokitiedostoa tietyn objektin käytöstä.

Windows NT:n tietoturva perustuu näihin periaatteisiin. Ajatuksena on ensin varmistaa (*Verify*), että käyttäjät ovat niitä, joiksi itseään väittävät kirjautumisen aikana ja sitten tarkistaa (*Authorize*) heidän käyttöoikeutensa. Tähän tarvitaan käyttäjätunnusta, joka sisältää tiedot siitä, keitä käyttäjät ovat ja mitä he saavat järjestelmässä tehdä.

Tehokas tietoturva on käytännössä mahdotonta muissa käyttöjärjestelmissä, kuten MS-DOS:issa, Windows 95:ssä, Macintoshissa ja OS/2:ssa. Ne on suunniteltu siten, että käyttäjät voivat käyttää järjestelmää lähes tai kokonaan ilman rajoituksia. Käyttöjärjestelmä on liian heikko voidakseen taata hyvän tietoturvallisuuden.

Windows NT sen sijaan on objektiorientoitunut käyttöjärjestelmä, ja sen tietoturvaominaisuudet on rakennettu objektirakenteen alimmalle tasolle. Tästä syystä Windows NT on helpompi turvata kuin lähes mikä tahansa muu käyttöjärjestelmä.

Windows NT käyttää hyväkseen Intel 80386- (ja tehokkaampien) prosessorien ominaisuuksia tietoturvaominaisuuksien toteuttamisessa. Muistin turvausominaisuudet estävät ohjelmia pääsemästä toisen ohjelman tai

itse käyttöjärjestelmän ohjelmakoodiin tai tietoihin. Jokaisella ohjelmalla on oma, suojattu muistinsa ja käyttöjärjestelmä estää ohjelman tai prosessin luvattomat yritykset tunkeuta toisen ohjelman tai prosessin muistiin.

Käyttäjätunnus (*User Account*) on keskeinen osa Windows NT -käyttöjärjestelmää. Jos joku haluaa käyttää tietokonetta tai verkkoa, hän joutuu ensin antamaan käyttäjätunnuksen ja salasanan. Käyttäjän kirjoittamat tiedot tarkistetaan **käyttäjätietokannasta** (*User Account Database*), joka sisältää käyttäjien tunnistukseen tarvittavat tiedot. Jos tiedot ovat oikein, käyttäjä pääsee verkkoon.

Windows NT:n tietoturva perustuu Yhdysvaltain puolustusministeriön kehittämiin turvallisuusohjeisiin. Tämä turvataso koskee yksittäisiä työasemia, mutta ei koko verkon turvallisuutta. Verkko on turvavaatimuksiltaan täysin erilainen ja paljon monimutkaisempi. Siihen liittyy koko joukko asioita, joita mikään yksittäinen käyttöjärjestelmä ei pysty hoitamaan (esimerkiksi tiedonsiirtoyhteyksien turvaaminen). Noudattamalla näitä ohjeita yksittäisille järjestelmille voidaan kuitenkin saavuttaa korkea turvallisuuden taso ja yksi askel kohti koko verkon turvaamista.

NT:n tietoturva tarjoaa tavan valvoa käyttäjien pääsyä järjestelmään. Sitä voidaan verrata yrityksen tai vaikkapa armeijan turvaluokituksiin. Windows NT käyttää **toimintavapauksien rajoittamia suojauksia** (*Discretionary Access Controls*), joiden avulla voidaan hallita täsmälleen, kutka käyttäjät saavat käyttää ja mitä. Esimerkiksi **Projektipäälliköt-ryhmällä** voi olla oikeudet muuttaa projektien tiedostoja, mutta **Projektijäsenet-ryhmällä** voi olla vain oikeudet lukea projektien tiedostoja.

Windows NT valvoo, kuka käyttäjä järjestelmään kirjautuu ja antaa sitten käyttäjälle oikeustodistuksen, jonka avulla käyttäjä voi käyttää järjestelmän turvattuja palveluja. Windows NT:ssä on siis eräänlainen kaksitasoinen suojausjärjestelmä:

1) Käyttäjällä täytyy ensinnäkin olla pääsy järjestelmän tiettyyn resurssiin -

2) ja sitten lisäksi resurssin täytyy sallia käyttö.

Ensimmäinen on **oikeus** (*Right*), jälkimmäinen **lupa** (*Permission*).

Käyttäjällä voi olla resurssin käyttöoikeus, mutta resurssilla täytyy olla käytön sallivat lupamääritykset. Windows NT:ssä on oikeuksia, joiden avulla käyttäjät voivat esimerkiksi varmuuskopioida järjestelmätiedostoja, sammuttaa järjestelmän, ladata ja poistaa laiteohjaimia (ajureita) ja hallita valvontalokeja.

Esimerkiksi kirjoittimen käyttöoikeudet voivat olla siten asetettu, että kuka tahansa voi ottaa kirjoittimen käyttöönsä, mutta vain joillakin käyttäjillä on oikeus hallita kaikkia kirjoittimen tulostustöitä.

Oikeuksia valvotaan **käyttäjätunnusten** (*User Account*) avulla. Käyttäjätunnusta voidaan Windows NT -ympäristössä verrata työntekijän tietoihin henkilöstöosastolla. Siinä on tiedot käyttäjästä ja hänen oikeuksistaan järjestelmässä. Käyttäjätunnukseen liittyy **yksilöllinen turvatunnus** (*Security Identifier*, SID), joka nähdään esimerkiksi **rekisterieditorilla** (**REGEDT32.EXE** tai **REGEDIT.EXE**) tai Resource Kitin **GETSID.EXE**:llä:

```
C:\>getsid \\v1 JKI \\v2 JKI
The SID for account VERSTAS\JKI matches account VERSTAS\JKI
The SID for account VERSTAS\JKI is
S-1-5-21-1289181413-810293876-390482200-1002
The SID for account VERSTAS\JKI is
S-1-5-21-1289181413-810293876-390482200-1002
```

Se kertoo mm. version (**S-1**), Windows NT:n (**5**) ja käyttäjätunnuksen hallinta-alueen (**21-1289181413-810293876-390482200**) sekä suhteellisen (**1002**) tunnuksen (*RID, Relative ID*).

Samalla käyttäjätunnuksella ei saa olla kahta SID:iä - tällainen tilanne syntyy, jos sama käyttäjätunnus luodaan erikseen esim. NT-työasemaan ja myös toimialueeseen.

Jos käyttäjän antama käyttäjätunnus ja salasana on oikein ja käyttäjällä on oikeus käyttää järjestelmää, käyttäjän kirjautuessa Windows NT:een luodaan **oikeustodistus** (*Access Token*) ja se myönnetään SID:n, ei käyttäjätunnuksen perusteella. Kaikki käyttäjän oikeusmääritykset tehdään tämän **oikeustodistuksen** avulla.

Se sisältää käyttäjän tunnistenumeron sekä niiden ryhmien tunnisteet, joihin käyttäjä kuuluu. Kun käyttäjä käyttää jotakin järjestelmän resurssia, oikeustodistuksen tietoja verrataan resurssin tietoihin käyttäjistä, joilla on lupa käyttää sitä.

Tässä vaiheessa kuvaan tulee mukaan kaksitasoinen turvallisuusjärjestelmä. Oikeusmääritykset (*Access Control Architecture*) määritellään **oikeuslistalla** (*ACL, Access Control List*). Jokaisella resurssilla on oikeuslistansa eli luettelo käyttäjistä, joilla on lupa käyttää sitä, ja luettelon tietoja verrataan käyttäjän **oikeustodistukseen**.

Ydin

Windows NT:n turvallisuuden tarjoavat komponentit muodostavat suojausalijärjestelmän. Tämäkin osa järjestelmää on kerrostettu: pohjalla on tietokoneen laitteisto ja ylimpänä sovellukset. Käyttäjä käyttää ylimmän tason komponentteja. Kaikki välissä olevat kerrokset turvaavat ylempiä kerroksia ja ovat yhteydessä alempiin kerroksiin.

Eräs Windows NT:n suunnittelun perusteista oli **siirrettävyys**. Siksi NT:lle on luotu hyvin pienen ydintason ohjelmamoduuli, **ydin** (*Kernel*), joka toimii kaikilla halutulla prosessoreilla. Jotta ohjelmistokehittäjien työ helpottuisi, on lisäksi luotu laitteistoeroavaisuudet ylemmiltä kerroksilta kätkevä *Hardware Abstraction Layer* (HAL). Näin eri laitteistot näyttäytyvät ohjelmistokehittäjille samanlaisina ja ohjelmia on helpompi kirjoittaa.

Koska Windows NT-käyttöjärjestelmää käytetään monenlaisissa käyttöympäristöissä (eikä niissä kaikissa tarvita kaikkia Windows NT:n ominaisuuksia), Windows NT on suunniteltu modulaariseksi - siihen voidaan lisätä osia tai poistaa niitä. Esimerkiksi käyttöliittymä on yksi moduuli (Internet Explorer 4.0). Nämä moduulit on helppo liittää ytimeen.

Ydin suunnittelee aikataulun prosessorissa ajettaville toiminnoille. Prosesseja kutsutaan **säikeiksi** (*thread*) ja ydin vastaa siitä, että prosessori ajaa näitä säikeitä. Ydin varmistaa, että tärkeimmät säikeet ajetaan ennen kuin vähemmän tärkeät säikeet. Lisäksi ydin tahdistaa siihen liittyvien komponenttien toimintoja:

- **Object Manager** - tiedostoja, kansioita, liitäntöjä, prosesseja ja säikeitä sanotaan tavallisesti objekteiksi. Object Manager vastaa niiden nimeämisestä, turvallisuudesta, jakamisesta ja poistamisesta

- **Process Manager** - komponentti, joka luo ja poistaa prosesseja
- **Virtual Memory Manager** - komponentti, joka luo levytilasta näennäismuistia
- **Local Procedure Call Facility** - apuväline, jonka avulla sovellukset kommunikoivat käyttöjärjestelmän alempien kerrosten kanssa viestinvälityskomponentin kautta
- **I/O Manager** - komponentti, joka hoitaa käyttöjärjestelmän ja ulkomaailman välisiä yhteyksiä. Se käsittelee **oheislaiteohjaimia** (*Device Drivers*) eli ajureita - käytännössä ohjelmistomoduuleja - joiden avulla käyttöjärjestelmä pääsee käsiksi fyysisiin laitteisiin kuten verkkoliitäntäkortteihin, levyasemiin ja välimuistiin.

Lisäksi tarvitaan suojauksista huolehtiva alijärjestelmä.

Windows NT tarjoaa nämä komponentit järjestelmänä, joka on rakennettu alhaalta ylöspäin. Siksi se on siirrettävä ja sen voi skaalata moniprosessorijärjestelmiin, se on **laajennettavissa** lisäämällä moduuleja tarpeen mukaan ja lisäksi se täyttää C2-turvallisuusvaatimukset.

Objektit

Windows NT:ssä esitetään melkein kaikki *objekteina*: tiedostot, muisti, laitteet, järjestelmäprosessit, säikeet ja jopa Työpöydällä näkyvät ikkunat. Objektit ovat Windows NT -käyttöjärjestelmän tietoturvan perusta:

- Objekti on itsenäinen kokonaisuus, joka sisältää omat tietonsa ja niiden hallintaan tarvittavat toiminnot
- Objekteja on monia erilaisia. Niiden ominaisuudet määrittyvät niiden objektityypin perusteella
- Windows NT:n objekteihin päästään ainoastaan itse käyttöjärjestelmän kautta ja tiukkojen turvatoimien jälkeen

- Turvajärjestelmä tarkistaa kaikki oikeudet käyttää objekteja, ja valvontajärjestelmä voi luoda tapahtumista lokitiedoston

- Objektin ulkopuolisen prosessin täytyy käyttää funktioita tietojen noutamiseen objektilta.

Sovelluksessa on tyypillisesti satoja tai tuhansia objekteja. Ylätasolla olevan objektin ei tarvitse välittää alempien kerrosten objekteista, jotka suorittavat omia tehtäviään saamiensa ohjeiden mukaisesti.

Turvallisuuteen tämä liittyy siten, että objektit kätkevät tiedon ulkomaailmalta ja antavat tietoja vain tietyillä tavoilla, jotka on määritetty objektin funktioissa. Näin ulkoiset prosessit eivät pääse suoraan käyttämään sisäisiä tietoja. Kaikki asiat Windows NT -käyttöjärjestelmässä ovat objekteja. Niinpä esimerkiksi datatiedostoa voi ajatella objektina, johon pääsyä rajoitetaan määrittämällä, kuka saa lukea sen.

Windows NT:n tietoturvallisuus on hyvä, koska järjestelmä ei koskaan anna **sovellusohjelmien** käyttää objekteja suoraan. Käyttöjärjestelmä antaa luvan kaikille objektiin kohdistuville toiminnoille ja suorittaa ne. Windows NT:n on melko helppo tarkistaa eri objekteihin kohdistuvien toimintojen oikeutus, koska objektit sisältävät itse suuren osan toimintojen hyväksymiseen tarvittavista tiedoista.

Suojausalijärjestelmä

Windows NT:n turvallisuudesta vastaava alijärjestelmä vaikuttaa koko Windows NT -käyttöjärjestelmään. Se muodostaa yhden yksittäisen järjestelmän, jonka kautta tarkistetaan kaikki yritykset käyttää objekteja, sisältäen levyllä olevat tiedostot, muistiprosessit ja liitännät lisälaitteisiin. Näin yksikään sovellus tai käyttäjä ei voi käyttää objekteja ilman kunnon oikeuksia. Alijärjestelmän komponentit ovat:

- **Local Security Authority** (LSA) - turvajärjestelmän keskeinen osa, joka luo oikeustodistukset, valvoo paikallisen tietokoneen turvakäytäntöjä ja tarkistaa kirjautuvien käyttäjien oikeudet

- **Logon Process** - prosessi joka hyväksyy sekä paikallisten että etäkäyttäjien kirjautumisen sisään

- **Security Accounts Manager** (SAM) - järjestelmä ylläpitää tietokantaa käyttäjistä, joilla on oikeus käyttää järjestelmää ja tarkistaa oikeudet kirjautumisprosessin aikana

- **Security Reference Monitor** (SRM) on NT:n **ytimen** (Kernel)-komponentti, joka estää objektien suoran käytön. Se tarkistaa oikeudet aina, kun objektia yritetään käyttää. SRM luo myös valvontaviestit.

NT:n hakemistotietokanta (*Directory Services*) voi verkkoympäristössä sijaita useilla eri tietokoneilla. Kun käyttäjä kirjautuu paikalliselle tietokoneelle, kyseisen palvelimen tai työaseman SAM hakee käyttäjätunnisteet tietokannasta. Windows NT -toimialueverkkoympäristössä käyttäjätietoja voidaan säilyttää yhden tai useamman palvelimen hakemistotietokannassa; näitä palvelimia kutsutaan toimialueen ohjauskoneiksi (*Domain Controller*) ja ne jakavat ja päivittävät käyttäjätunnuksiin liittyviä tietoja. Tämän jaetun tietokannan ansiosta käyttäjä voi käyttää koko verkon resursseja yhdellä kirjautumisella.

Kirjautuminen

Kirjautuminen Windows NT -järjestelmään alkaa käyttöjärjestelmän käynnistämisellä uudelleen tai painamalla näppäinyhdistelmää **Ctrl+Alt+Del**, jolloin käynnistyy uusi kirjautuminen.

Näppäinyhdistelmä **Ctrl+Alt+Del** suojaa muuten Troijan hevosilta, jotka naamioituvat käyttöjärjestelmäksi ja yrittävät huijata käyttäjän kirjoittamaan käyttäjätunnuksensa ja salasanansa. Tällainen kirjautumissuojaus on käytössä vain Windows NT -käyttöjärjestelmissä.

Ctrl+Alt+Delillä varmistetaan myös se, että hyväksyttävä Windows NT -kirjautumistoiminto käynnistyy. Tätä näppäinyhdistelmää täytyy käyttää aina kirjauduttaessa jo käynnissä olevalle koneelle.

Koska jokainen käyttäjä kirjautuu tietokoneelle erikseen, käyttäjät voivat luoda koneelle omat työpöytäasetuksensa. Kun käyttäjä kirjautuu tietokoneelle, edellisen istunnon asetukset noudetaan käyttäjäprofiilista ja palautetaan voimaan.

Netlogon-palvelu tarjoaa käyttäjille mahdollisuuden kirjautua toimialueelle miltä tahansa tietokoneelta. **Netlogon** kopioi turvatietokannan muutokset kaikille toimialueen ohjauskoneille, jolloin käyttäjät voivat kirjautua sisään miltä tahansa ohjauskoneelta. Netlogon-palvelu toimii kaikilla toimialueeseen kuuluvilla Windows NT -tietokoneilla, myös NT-työasemissa.

Windows NT:n kirjautumisprosessi on seuraavanlainen:

1) Kun kirjautumisnäyttö tulee esille, käyttäjä antaa siihen käyttäjätunnuksensa ja salasanansa sekä sen työaseman tai toimialueen nimen, johon hän haluaa kirjautua. Käyttäjä tunnistetaan käyttäjätunnuksen perusteella ja salasanaa käytetään kirjautumisen hyväksymiseen

2) **Local Security Authority** (LSA) ajaa oikeuksien tarkistamisohjelman. Oikeuksien tarkistamisohjelma voi olla Windows NT:n apuohjelma tai jokin erikseen hankittu ohjelma

3) Jos käyttäjä haluaa kirjautua paikalliselle tietokoneelle, oikeuksien tarkistamisohjelma pyytää LSA:ta tarkistamaan, löytyvätkö käyttäjätunnus ja salasana paikallisesta hakemistotietokannasta. Jos käyttäjä haluaa kirjautua toimialueelle, oikeuksien tarkistamisohjelma lähettää tiedot edelleen toimialueen ohjauskoneelle, ja oikeuksien tarkistaminen tapahtuu Netlogon-palvelun kautta

4) Paikallinen tai toimialueen SAM palauttaa käyttäjän turvatunnuksen, jos käyttäjätunnus hyväksytään. SAM antaa myös tietoja esimerkiksi oikeuksista, kotihakemiston sijainnista ja kirjauskomentojonoista (*Logon Script*)

5) LSA luo **oikeustodistuksen** (*Access Token*), joka sisältää käyttäjän **turvatunnuksen** (*Security Identifier*, SID), käyttäjän ryhmän turvatunnukset sekä oikeudet, jotka käyttäjällä on paikalliseen järjestelmään. Windows NT seuraa ja valvoo eri käyttäjien käyttämien ohjelmien lupia **subjektien** avulla. Subjekti on yhdistelmä käyttäjän oikeustodistuksesta ja ohjelmasta, joka toimii käyttäjän asemesta. Käyttäjän puolesta esiintyvät ohjelmat tai prosessit ajetaan käyttäjän suojausympäristössä (*Security Context*), joka valvoo, mitä oikeuksia subjektilla on objekteihin tai järjestelmäpalveluihin

6) Kirjautumisen lopuksi luodaan subjekti ja ajetaan tarvittavat ohjelmat. Tässä vaiheessa järjestelmä on tunnistanut käyttäjän ja käyttäjä voi alkaa käyttää objekteja niiden käyttölupien mukaisesti.

Toimialueissa käyttäjä tunnistetaan toimialueen **pääohjauskoneella** (*Primary Domain Controller*) tai **vara-ohjauskoneella** (*Domain Controller*), joka sisältää kopion hakemistotietokannasta. Käyttäjät voivat kirjautua joko NT-työaseman paikallisella käyttäjätunnuksella, tai kirjautua toimialueelle.

Tämä riippuu siitä, mitä käyttäjä valitsee kirjautumisnäytön **Domain**-kenttään:

- Jos käyttäjä antaa Domain-kenttään paikallisen NT-työaseman nimen, NT-työasema antaa käyttäjän kirjautua paikalliseen järjestelmään

- Jos käyttäjä valitsee Domain-kenttään jonkin toimialueen nimen, tapahtuu etäkirjautuminen (*Remote logon*), jossa kirjautumispyyntö lähetetään paikalliselle toimialueen ohjauskoneelle tarkistettavaksi. Jos annettu toimialue ei ole paikallinen toimialue, toimialueen ohjauskone lähettää pyynnön edelleen annetun toimialueen ohjauskoneelle.

Toimialueen valvontakoneet tarkistavat käyttäjätunnuksen ja salasanan vertaamalla niitä hakemistotietokannan tietoihin. Jos tiedot ovat oikein, tunnistetiedot lähetetään takaisin kirjautumistietokoneelle sen toimialueen ohjauskoneen kautta, joka käyttäjätietoja alunperin yritti tarkistaa.

Jos tavallinen kirjautuminen epäonnistuu, käyttäjälle annetaan pääsy **Guest** (Vieras) -tunnuksella. Näin tapahtuu kuitenkin vain, jos Guest-käyttäjätunnus on käytössä ja salasanaa sen käyttöön ei tarvita. Oletuksena Guest-tunnus on käytettävissä Windows NT 4.0 -työasemissa, mutta ei Windows NT 4.0 -toimialueilla.

Kun käyttäjä on jo kirjautunut järjestelmään ja yrittää käyttää muilla tietokoneilla olevia resursseja, alkuperäiseen kirjautumiseen käytetyt tiedot lähetetään edelleen uudelle palvelimelle, joka niiden perusteella tarkistaa käyttäjän oikeudet. Tästä käytetään nimitystä **välitetty auktorisointi** (*Pass Through Authentication*) ja sen ansiosta käyttäjän ei tarvitse erikseen kirjautua jokaiseen uuteen resurssiin, jota hän haluaa käyttää.

Käyttöoikeusluettelot

Windows NT:ssä käsitellään kaikki aina objekteina, tiedostoista säikeisiin. Kukin objekti voidaan suojata **erikseen** tai **ryhmänä**. Objekteilla on erityyppisiä **lupia** (*Permissions*), joiden avulla ne voivat **sallia** (*Grant*) tai **kieltää** (*Deny*) niiden käytön.

Esimerkiksi hakemisto- ja tiedosto-objekteilla voi olla luku-, kirjoitus- ja suoritusluvat, tulostusjonoilla taas dokumenttien hallintalupa ja tulostuslupa. **Hakemistot** ovat tiedostoja sisältäviä kansio-objekteja, joten kansiolle myönnetyt luvat **periytyvät** (*Inherit*) sen sisältämille tiedosto-objekteille.

Käyttöoikeudet ja käyttäjätunnukseen liittyvät oikeudet ovat Windows NT:ssä kaksi eri asiaa. **Käyttäjätunnusmenetelmän** avulla tunnistetaan ja hyväksytään käyttäjä, **käyttöoikeuksilla** (*User Rights*) taas rajoitetaan käyttäjän oikeuksia käyttää eri objekteja.

Kaikilla objekteilla on **suojauskuvaus** (*Security Descriptor*), jossa kuvaillaan niiden turvaominaisuudet:

- Objektin omistajan **turvatunnus** (*Security ID*, SID). Omistaja on tavallisesti käyttäjä, joka on luonut objektin
- **Käyttöoikeusluettelo** (*Access Control List*, ACL) sisältää tiedot siitä, millä käyttäjillä ja ryhmillä on oikeus käyttää objektia
- **Järjestelmä-ACL** (*System ACL*) , joka liittyy valvontajärjestelmään
- **Ryhmäturvatunnus** (*Group Security ID*), jota käytetään UNIX-ympäristöä muistuttavassa POSIX-alijärjestelmässä.

ACL:ssä piilee asian ydin. ACL on luettelo käyttäjistä ja ryhmistä, joilla on lupa käyttää jotain objektia. Jokaisella objektilla on oma ACL:nsä.

Objektien omistajat voivat syöttää asetuksia ACL:ään esimerkiksi **File Managerin** (Tiedostojenhallinta, Windows NT 3.51) kaltaisten työkalujen avulla tai määrittämällä tiedostojen ja kansioiden **ominaisuuksia** (Properties, NT 4.0:ssa). Muita lupien määrittämiseen käytettäviä välineitä ovat Ohjauspaneelin **Network** (Verkko)- ja **Services** (Palvelut)-sovellukset.

Käyttäjistä voi olla objektin oikeusluettelossa useita eri merkintöjä, joiden avulla he saavat eritasoisia käyttöoikeuksia. Käyttäjällä voi esimerkiksi olla oman käyttäjätunnuksensa perusteella lukuoikeus tiedostoon ja ryhmän jäsenyyden perusteella luku- ja kirjoitusoikeus. Kukin lupa luetellaan erillisenä tietona ACL:ssa.

Kun käyttäjä yrittää käyttää objektia, hänellä on tavallisesti tietty esimerkiksi sovelluksessa tarvittava käyttöoikeus, kuten lukuoikeus tai luku- ja kirjoitusoikeus. **Security Reference Monitor** (SRM) myöntää tai kieltää pääsyn vertaamalla käyttäjän **oikeustodistusta** (*Access Token*) ACL:n tietoihin.

Koska oikeustodistus sisältää turvatunnuksen ja luettelon ryhmistä, joihin käyttäjä kuuluu, SRM vertaa näitä tietoja yhteen tai useampaan ACL:n merkintään, kunnes se löytää **riittävät oikeudet** pääsyn myöntämiseen. Jos se ei löydä riittäviä oikeuksia, pääsyä ei myönnetä.

Jos SRM löytää käyttäjästä useita merkintöjä, se tarkastelee jokaista niistä erikseen nähdäkseen, onko yksittäinen ACL:n asetus tai asetusyhdistelmä sellainen, että käyttäjä saa oikeuden käyttää objektia.

Esimerkiksi käyttäjä **JORND** kuuluu ryhmiin **Users**, **Gurut** ja **Everyone**. ACL:n asetukset tiedostolle **THUNDER.DOC** ovat seuraavat:

1. **Users**-ryhmän lukuoikeus
2. **Everyone**-ryhmän lukuoikeus
3. **Gurut**-ryhmän luku- ja kirjoitusoikeus
4. Käyttäjän **JORND** luku- ja kirjoitusoikeus

Kun käyttäjä **JORND** pyytää luku- ja kirjoitusoikeuksia tiedosto-objektiin, SRM vertaa käyttäjän **JORND** oikeustodistusta tiedoston ACL:ään. Ensin tarkistetaan ensimmäinen asetus, jolloin SRM huomaa, että **Users**-ryhmällä on **lukuoikeus** ja käyttäjä **JORND** on ryhmän **Users** jäsen. **JORND** on kuitenkin pyytänyt luku- ja kirjoitusoikeuksia tiedostoon **THUNDER.DOC**, joten SRM tarkistaa seuraavan tiedon ja saa saman tuloksen. Asetus 3 antaa halutun vastauksen, koska **JORND** kuuluu **Gurut**-ryhmään, ja on pyytänyt luku- ja kirjoitusoikeutta **THUNDER.-DOC**-tiedostoon.

Asetusta 4 ei nyt tarvita, koska asetus 3 täyttää turvavaatimukset. **No Access**-lupa estää kuitenkin kaikki yritykset käyttää objektia, vaikka käyttäjällä voi olla käyttöoikeuksia ACL:n muiden tietojen kautta. Jotkin ACL:n tiedot saattavat siis luvan myöntämisen sijaan kieltää pääsyn objektiin.

Windows NT:n suojausmenetelmiä

Windows NT:ssä on useita mahdollisuuksia hallita järjestelmän suojauksia. Suojaukset täyttävät USA:n puolustusministeriön (*Department of Defense*) standardin **C2**, jonka keskeisiä vaatimuksia ovat seuraavat:

- Käyttäjän identifioiminen kirjautumisen yhteydessä
- Prosessien käsittelemien objektien eristäminen muilta prosesseilta
- Objektin omistajan (*Owner*) on pystyttävä seuraamaan objektin käyttöä
- Järjestelmän vastuuhenkilöiden on pystyttävä valvomaan järjestelmän tapahtumia ja rajoittamaan tapahtumalokin käsittelyä
- Järjestelmän on pystyttävä suojautumaan ulkopuolisilta murtautumisyrityksiltä.

Käyttäjän oikeuksiin vaikuttavia suojauksia voidaan käsitellä Windows NT:n seuraavilla menetelmillä.

Käyttäjien hallinnalla (User Manager) ja **User Manager for Domains:lla** määriteltävät suojaukset:

- **Tilikäytäntö** (Account Policy)
- **Käyttöoikeuskäytäntö** (User Rights)
- **Valvontakäytäntö** (Audit Policy).

NTFS-levyllä voit määritellä käyttöoikeuksia:

- **Kansion käyttöoikeudet** (Directory Permissions)
- **Tiedoston käyttöoikeudet** (File Permissions)

Verkkoon jaetuille resursseille voit määritellä käyttöoikeudet:

- **Käyttöoikeudet jaetuille resursseille** (Access Through Share Permissions)

Lisäksi voit **rajoittaa käyttäjän ympäristöä**:

- **Järjestelmäkäytännöillä** (*System Policy*)
- **Profiileilla** (*Profiles*), varsinkin **pakollisilla** (*Mandatory*) profiileilla.

Näistä muodostuvat:

- **Käyttäjätunnuksen oikeudet**
- **Käyttäjäryhmien oikeudet**.

Suojausmenetelmiä

- NT:n omat mahdollisuudet:
  - Kirjautumisauktorisointi
  - Työaseman lukitus
  - Kirjautumissanoma
  - Käyttöliittymän rajoitukset
  - Käyttäjäprofiilit
  - Käyttöoikeudet
  - Tiedosto- ja hakemistotason suojaukset
  - NTFS-tason suojaukset
  - Käyttöoikeuskäytännöt
  - Sisäänrakennetut paikalliset ryhmät
  - Toimialueet ja luottosuhteet
  - RAS:n takaisinsoittoasetukset
- Muita suojauksia:
  - Salakirjoitus (kolmannen osapuolen)
  - Levykeaseman, näppäimistön ja virtakytkimen lukitseminen
  - Suojaus/Salakirjoituslaitteet, suojausisäntä (Security Host)
  - Serverihotellit, suojattu kaapelointi
  - Virtapiikkien estäminen, UPS

Valvontatyökalut

- Windows NT 4.0-työaseman mukana:
  - Levyn hallinta (Disk Manager)
  - Varmuuskopiointi (NT Backup)
  - **Käyttäjien hallinta (User Manager)**
  - **Resurssien valvonta (Performance Monitor)**
  - **Tapahtumien valvonta (Event Viewer)**
  - **Etäkäytön hallinta (Remote Access Admin)**
  - Windows NT Diagnostiikka (Windows NT Diagnostics)
- Windows NT 4.0-palvelimen mukana:
  - **Server Manager**
  - **User manager for Domains**
  - Remoteboot Manager
  - WINS Manager, DHCP manager
  - **System Policy Editor - Järjestelmäkäytäntöjen editori**
  - CD-ROM:milla e.m. valvontatyökalut sekä Win95- ja NT 4.0-työasemille

Muita työkaluja

- **Rekisterieditorit:**
  - REGEDT32, REGEDIT
  - Myös POLEDIT.EXE
- **Komentorivin komennot:**
  - CONVERT
  - NET CONFIG SERVER
- **Tiedostonhallinta (File Manager)**
- **SNMP**
- **Ohjauspaneeli (Control Panel):**
  - Järjestelmä (System)
  - Verkko (Network)
- **Resource Kit:**
  - C2 Configuration Manager
  - Shutdown Manager
  - Browser Monitor, Domain Monitor
  - Network Watch, Process Viewer
- Virustorjuntaohjelmat
- Varmuuskopiointiohjelmat
- Oma älli ja logiikka sekä kokemus:
  - **You don t need experience if you ve got attitude** ei päde NT-ympäristön hallinnassa

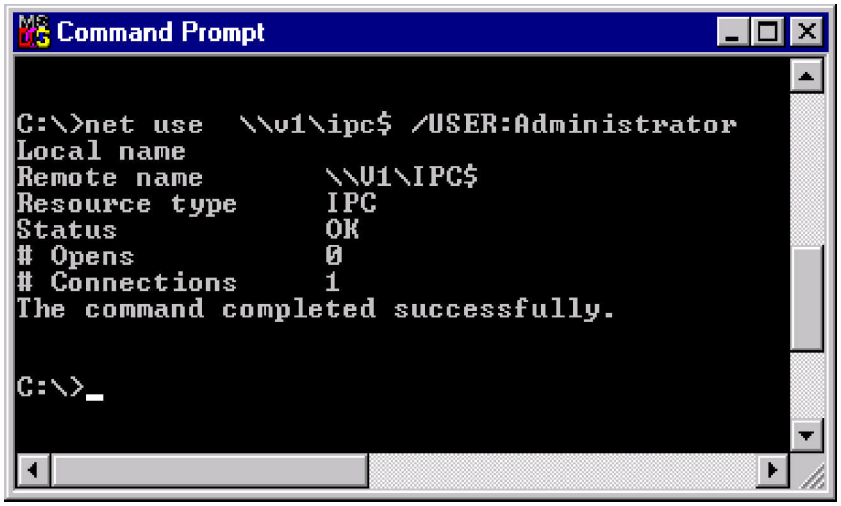
Valvontatyökalujen käytön edellytykset

Pääkäyttäjätason (Administrators-ryhmän jäsen) tunnuksella tulisi aina pystyä hallinnoimaan kohdetta NT-verkossa. Edellytys on tietysti, että käyttäjätunnus kuuluu **kohteessa paikalliseen Administrators-ryhmään**.

Myös muihin ryhmiin kuuluvilla käyttäjätunnuksilla (Server Operators, Account Operators jne) on ryhmäjäsenyyden edellyttämä oikeustaso kohdekoneessa.

Jos valvontatyökalu ei toimi oikein tai yhteyttä kohteeseen ei saada, kokeile komentorivin komentoa:

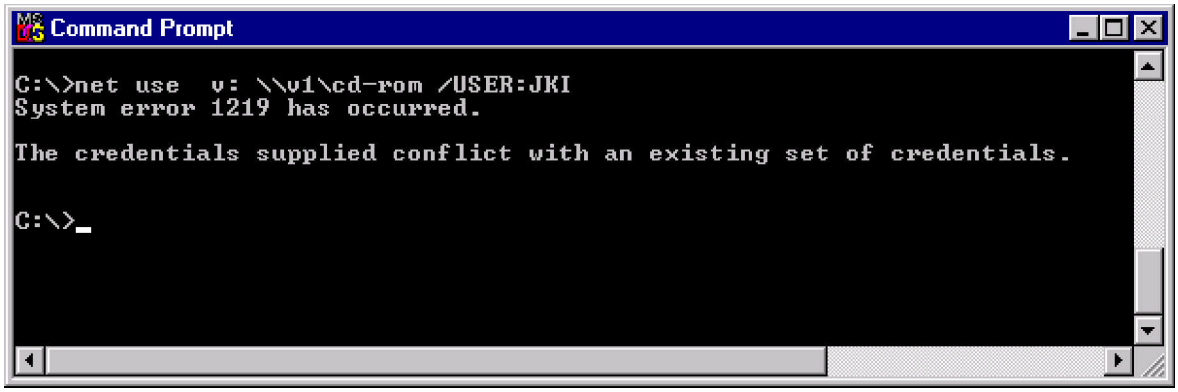
NET USE \\[kohde]\IPC$



Jos tämän komennon vastaus **ei** ole **The command completed successfully**, oikeudet eivät ole riittävät tai kyseessä voi olla verkkotason ongelma.

Voit myös kokeilla **NET USE**-komennon valitsinta **/USER**, jolla voit muodostaa yhteyden kohteeseen jollakin paikallisella käyttäjätunnuksella.

Jos saat ilmoituksen **The credentials supplied conflict with an existing set of credentials**, se tarkoittaa, että olet jo muodostanut yhteyden kohteeseen jollakin toisella käyttäjätunnuksella.



Kokeile tällöin komentoa

NET USE * /D

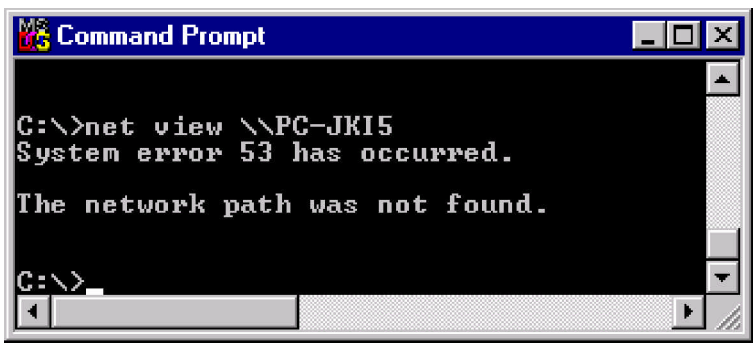
joka purkaa **kaikki** verkkoyhteydet.

Onko kohde ylipäätään verkossa saadaan selville komennolla:

NET VIEW \\[kohde]

Se ohittaa selauspalvelun (*Computer Browser*). Vastaus voi olla jokin seuraavista:

- **Listaus jaetuista resursseista** (sekä **The command completed succesfully**)
- **Access Denied** (joka sekin tulee kohteesta)
- **System error 53**, jolloin kohdetta ei verkosta löydy.



Kirjautumisohjeet ja menettelytavat

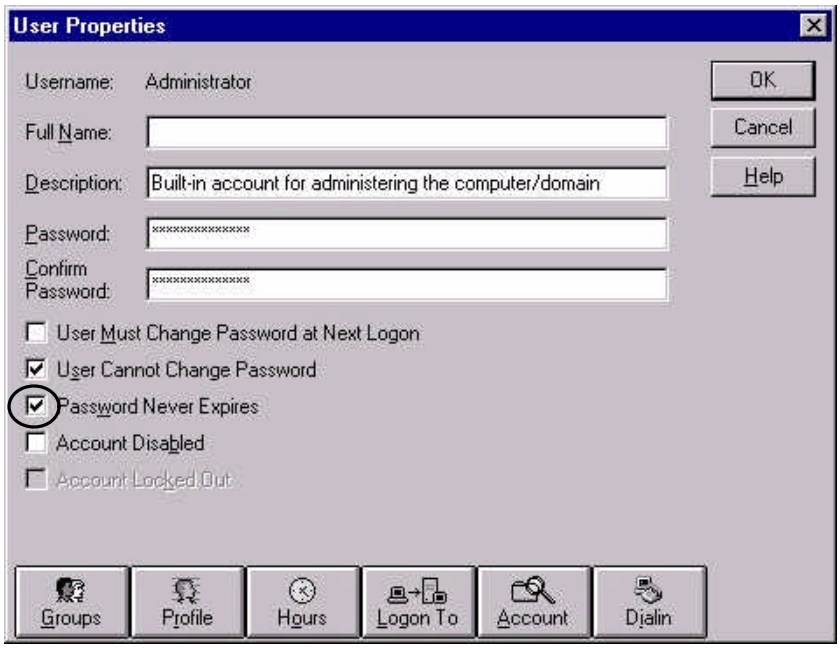
Kirjautumisprosessi on mahdollinen turvallisuusriski. Varoita käyttäjiä ja pyydä heitä suojelemaan salasanaansa ja olemaan varovaisia, kun he antavat salasanan kirjautumisen yhteydessä. *Joku voi aina katsella selän takana*.

Eri kirjautumisvaihtoehdot riippuvat siitä, onko työasema liitetty työryymään vai toimialueelle, myös kirjautuminen puhelinverkkoyhteyden (Dial Up Networking) kautta on mahdollista. Kirjautuminen tehdään sinne missä käyttäjän käyttäjätunnus on määritelty. Valinnat löytyvät toimialue-listasta **Domain** kirjautumisen yhteydessä ja seuraavilla käyttäjätunnuksilla voi kirjautua:

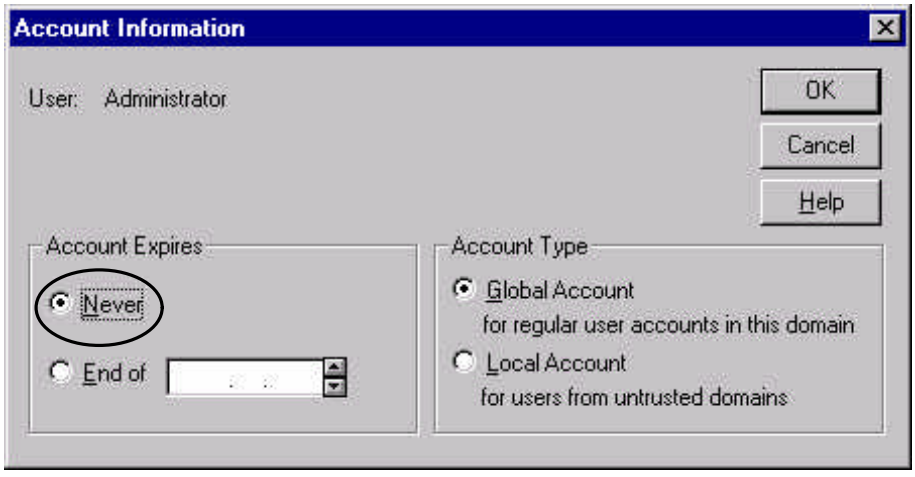
- Paikallinen käyttäjätietokanta: **Konenimi\Käyttäjätunnus**
- Toimialueen käyttäjätietokanta: **Toimialue\Käyttäjätunnus**
- Luotetun toimialueen käyttäjätietokanta: **Toimialue\Käyttäjätunnus**.

Periaatteita:

- Ota käyttöön salasanaohjeet. Vaihda salasanoja usein ja vältä salasanoja, jotka on helppo arvata. Älä koskaan kirjoita salasanoja ylös paperille
- Kirjaudu pois järjestelmästä poistuessasi työasemasi luota, tai käytä Windows NT:n näytönsäästäjää salasanalla suojattuna. Yllätyksien välttämiseksi tukihenkilöiden pitäisi välttää turhaa kirjautumista Administrator-tunnuksella ja käyttää **Domain Users/Users-tason** käyttäjätunnusta normaalityöskentelyssä



- Administrator-tason käyttäjätunnusten salasanan ei tulisi koskaan vanheta (Password Never Expires)!

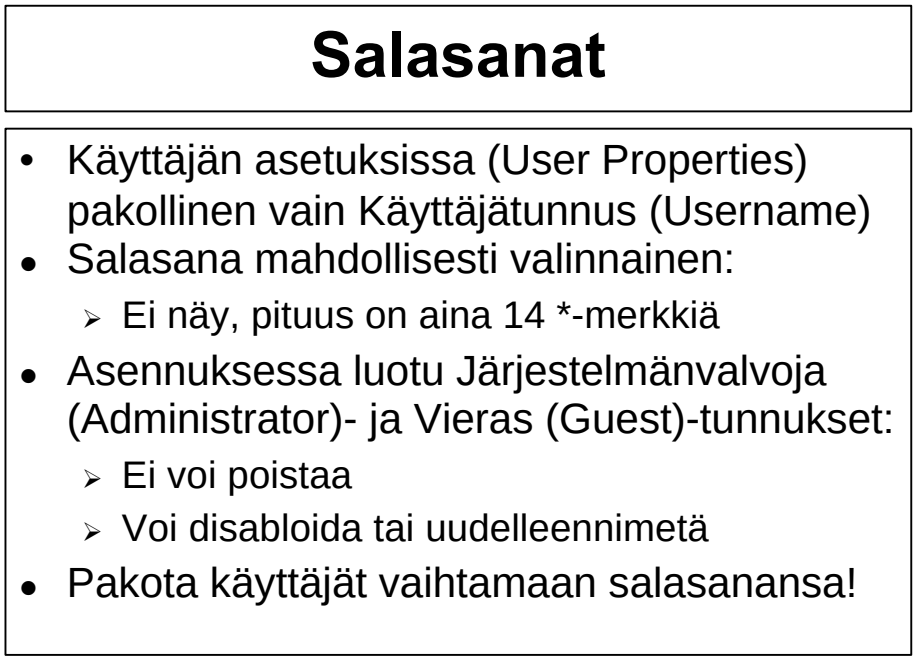


- Administrator-tason käyttäjätunnusten kirjautumisaikoja ja -työasemia ei tulisi rajoittaa!

- Älä kirjaudu pääkäyttäjien tunnuksilla vieraissa ympäristöissä sijaitsevilta työasemilta, esimerkiksi internetin kautta. Kirjoitumista voidaan valvoa, jopa valvoa piilotetuilla kameroilla tai muilla laitteilla. Lisäksi virukset voivat päästä kriittisiin järjestelmätiedostoihin

- Voit vaihtoehtoisesti luoda *pomminvarman* Administrator-tunnuksen, jossa kahdella tai useammalla käyttäjällä on osa sekä käyttäjätunnuksesta että salasanasta, ja kaikkien täytyy olla paikalla tunnusta käytettäessä. Kaikkihan olemme nähneet agenttileffoja...

- Kyseenalaisissa tapauksissa näytä käyttäjille tiedot heidän viimeisestä kirjautumiskerrastaan, jotta he voivat itse havaita, jos joku muu on käyttänyt tunnusta.



ScanNT

ScanNT on apuohjelma, jolla voi yrittää murtaa NT:n salasanoja. Sen periaate on kokeilla erilaisia yksinkertaisia salasanoja, jolloin saadaan selville ovatko salasanat liiankin yksinkertaisia.

ScanNT kokeilee 10.000 salasanaa minuutissa (Pentium/100 MHz, 24 Mt RAM), tutkittavien käyttäjätunnusten määrä on rajoittamaton.

Lisätietoja: **http://www.ntsecurity.com/Products/ScanNT**

Samaa raa an voiman menetelmää käyttävät varsinaiset salasanojen murtamiseen tarkoitetut ohjelmat, kuten **PWdump** ja **NTCrack**.

Passprop

Resource Kitin **Passprop**-apuohjelmalla voidaan tehdään yksinkertaisia salasanoihin liittyviä asetuksia ja tarkistuksia.

Syntaksi on

PASSPROP [/complex] [/simple] [/adminlockout] [/noadminlockout]

Parametrit:

/complex	Salanojen on oltava monimutkaisia, sekoitus pieniä ja isoja kirjaimia sekä numeroita
/simple	Salasanat voivat olla yksinkertaisia
/adminlockout	Administrator-käyttäjätunnus voidaan lukita (tunnuksella voi silti kirjautua ohjauskoneilla (*Domain Controller*)
/noadminlockout	Administrator-käyttäjätunnusta ei voi lukita

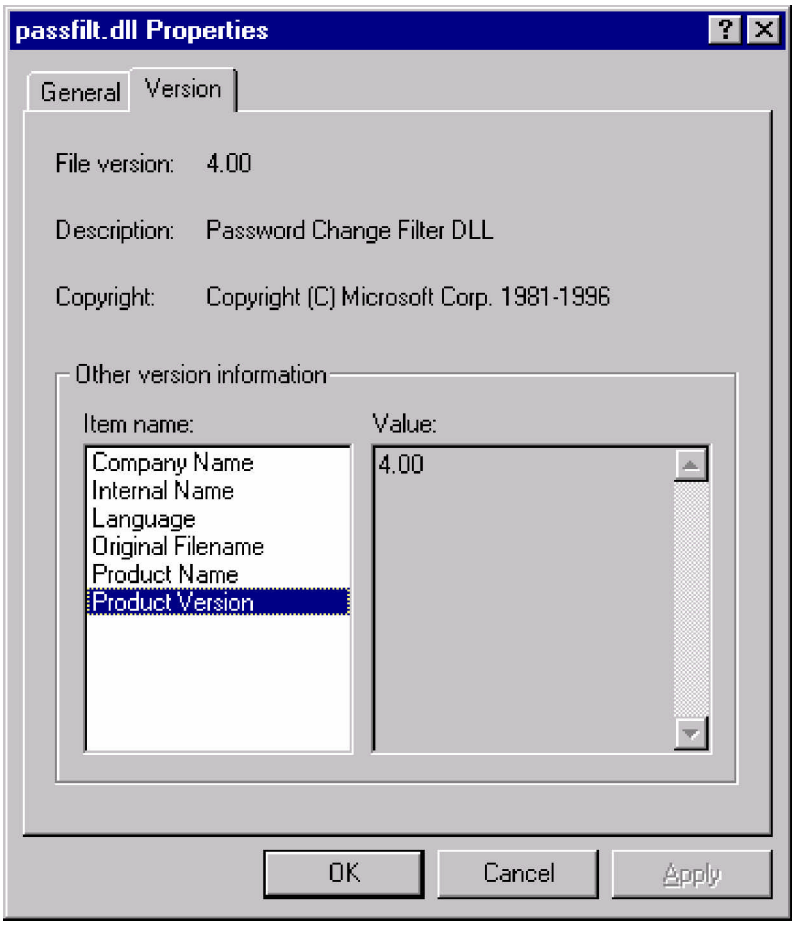
Lisäasetuksia voi tehdä **User Manager for Domainsilla** tai **NET ACCOUNTS**-komennolla.

Passfilt

NT:ssä on mahdollista ottaa käyttöön ns. **vahvat salasanat** (*Strong Passwords*). Windows NT 4.0:n **Service Pack 2** sisältää **Passfilt.dll**-tiedoston, jolla voidaan tehostaa salasanojen vaatimuksia:

- Salasanojen on oltava vähintään 6 merkkiä pitkiä
- Salasanassa on oltava vähtinään kolme merkkiä seuraavista neljästä luokasta: **isot kirjaimet** (A, B, C, ... Z), **pienet kirjaimet** (a, b, c, ... z), **numerot** (0, 1, 2, ... 9) ja **erikoismerkit**
- Salasana ei voi sisältää käyttäjätunnuksen tai käyttäjän nimen osaa.

Asetuksia ei voi muuttaa esimerkiksi rekisteristä.



Jotta asetukset tulevat käyttöön, kaikissa NT-palvelimissa (**ohjauskoneet** eli *Domain Controllerit* ja *Stand-Alone Serverit*) tehdään seuraava käyttöönotto:

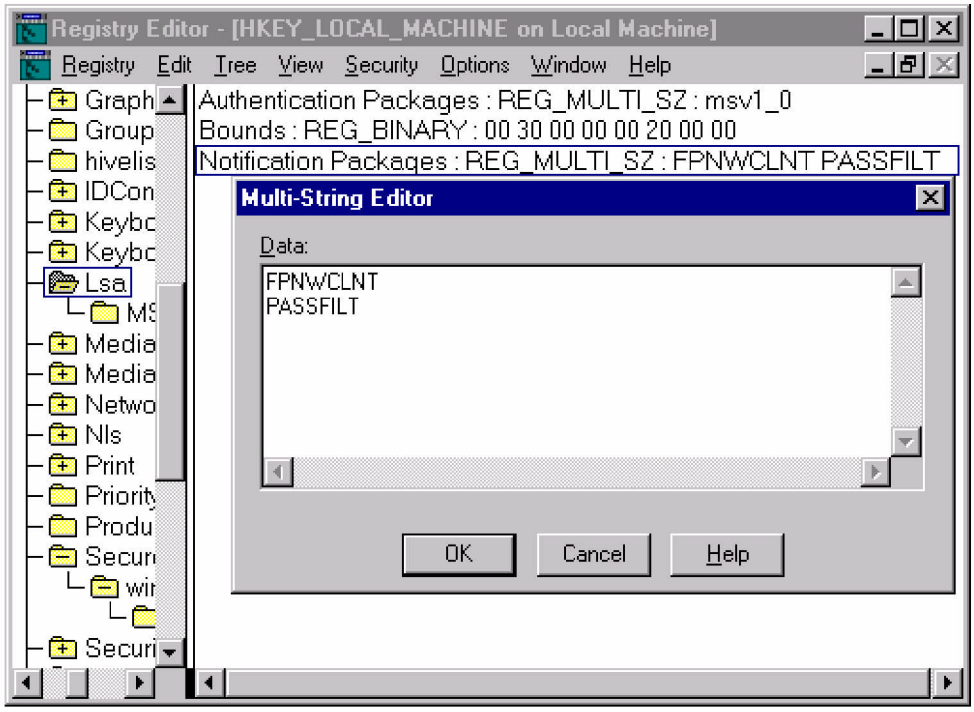
1) Asenna Windows NT 4.0 **Service Pack 2** tai **Service Pack 3**

2) Kopioi **Service Packin** asennushakemistosta **Passfilt.dll %SYSTEMROOT%\SYSTEM32** -hakemistoon

3) Käytä **REGEDT32.EXE**-rekisterieditoria: lisää nimi **Notification Packages**, tyyppi on **REG_MULTI_SZ**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Lsa**
Nimi	**Notification Packages**
Tyyppi	**REG_MULTI_SZ**
Arvo	**PASSFILT**

4) Jos arvo **FPNWCLNT** on jo olemassa, lisää **PASSFILT** sen alle:



5) Sulje editori ja käynnistä NT-palvelin uudelleen.

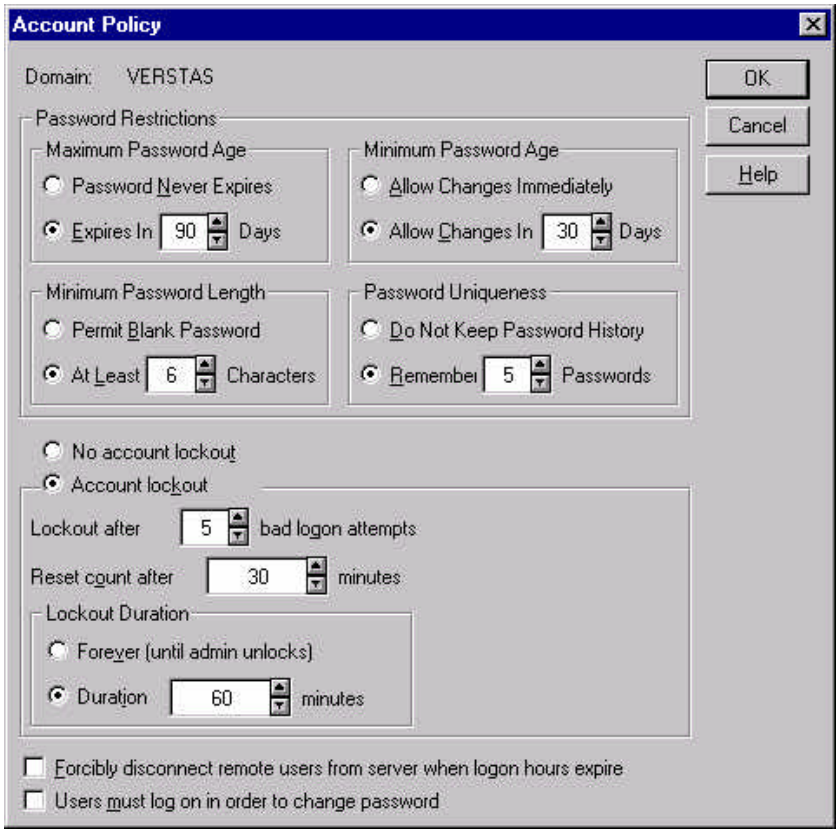
Käyttäjätunnukset ja -ryhmät

Periaatteita käyttäjätunnusten ja -ryhmien asetuksille:

- Pääkäyttäjillä täytyy olla kaksi käyttäjätunnusta; laajemmilla käyttöoikeuksilla varustettu tunnus järjestelmän hallintaa varten ja rajatuilla oikeuksilla varustettu tunnus muuta käyttöä varten

- Vaihda Administrator-tunnukselle jokin toinen, vaikeasti arvattava nimi

- Määritä käyttäjätunnuksille lukitus kirjautumisen epäonnistuessa, jotta tietoturvallisuus ei vaarantuisi



- Käytä **Account Policy** -asetuksia; esimerkiksi salasana päättyy 60:ssa päivässä, saa muuttaa 30 päivän jälkeen - minimipituus 6 merkkiä, 10 ainutkertaista salasanaa. Huomioi myös käyttäjätunnuksen lukitseminen ja käyttäjän istunnon pakotettu katkaisu toimialueella

- Estä käyttö tai poista käytöstä (*Disabled*) käyttäjätunnus, kun työntekijä lähtee pois yrityksen palveluksesta

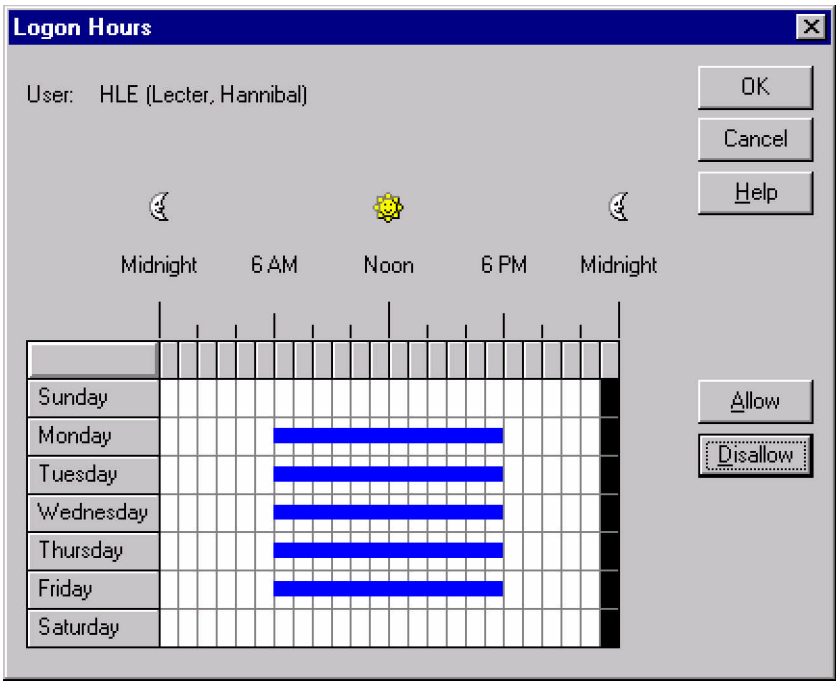
- Käyttäjillä pitäisi olla oikeudet vain niihin toimintoihin, joita he tarvitsevat tehtäviensä tekemiseen. Määritä käyttäjätunnuksille mahdollisimman vähän oikeuksia

- Estä **Guest**-tunnuksen käyttö, tai jos haluat pitää sen käytössä, tarkista, mihin toimintoihin sen käyttö oikeuttaa. Tarkista tunnuksen asetukset paitsi toimialueilla, myös Windows NT-työasemissa!

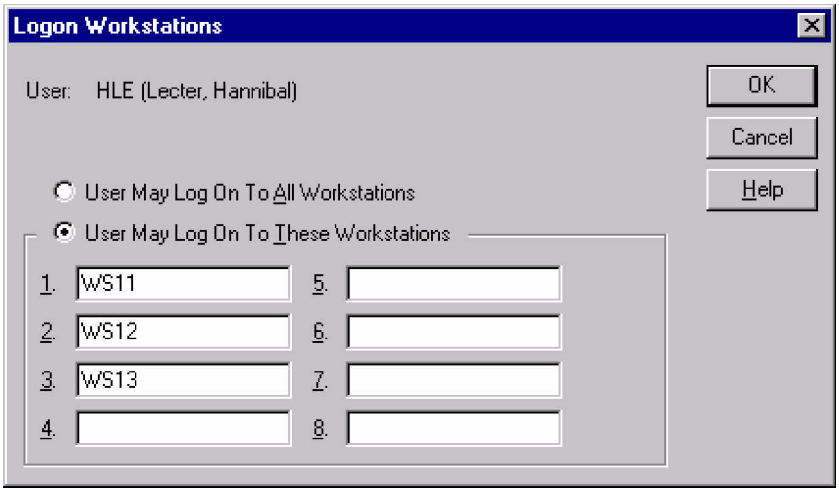
- Älä pidä missään järjestelmän osassa tarpeettomia käyttäjätunnuksia

- Määritä varmuuskopiointia ja tulostuksenhallintaa varten erilliset pääkäyttäjät. Käytä hyväksesi valmiita **Backup Operators**- ja **Print Operators**-ryhmiä

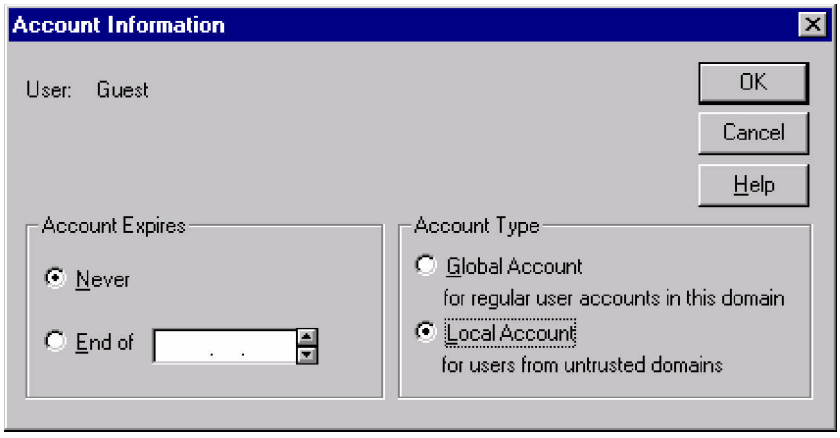
- Määrittele tarvittaessa **Logon Hours** - milloin käyttäjä saa kirjautua toimialueelle. Tämän saa vielä tiukemmaksi pakottamalla käyttäjän kirjautumaan toimialueelta, kun kirjautumisaika päättyy (**Forcibly disconnect remote users from server when logon hours expire**)



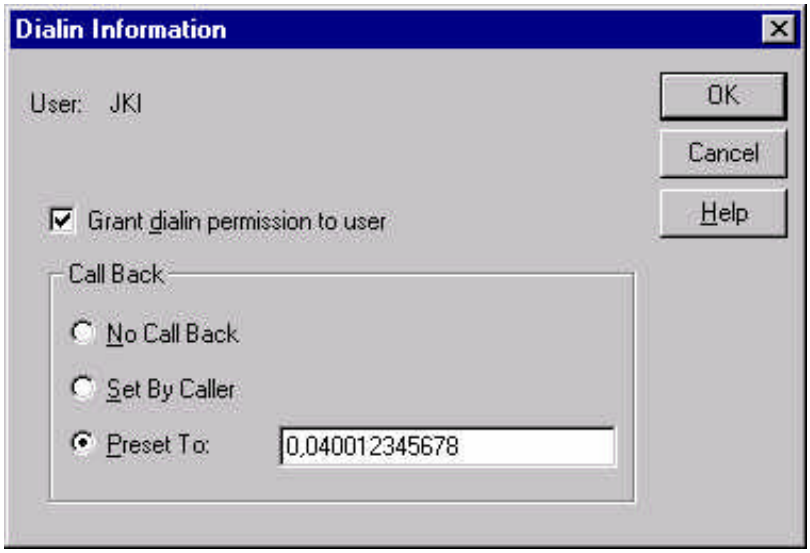
- Määrittele tarvittaessa **Logon Workstations** - miltä työasemilta käyttäjä saa kirjautua toimialueelle. Asetus koskee myös Windows 95-työasemia!



- Määrittele tarvittaessa **Account Expires** - milloin käyttäjätunnuksen voimassaolo päättyy - oletuksena ei koskaan (**Never**). Käyttäjätunnus voidaan myös määritellä toimialueen paikalliseksi käyttäjätunnukseksi: ei näy edes saman toimialueen NT-työasemissa, eikä ole käytettävissä luottosuhteen kautta.



- Määritä etäkäyttöpalvelun takaisinsoittoasetuksissa **Dialin Information** pakollinen ennalta-annettuun numeroon **Preset to** - muista ulkolinjan (esim. 0) ja viiveen (,) asetukset sekä GSM-datapuhelun numero (joka on eri kuin puhelimen numero).



Guest

Guest (Vieras)-käyttäjätunnusta käytetään tilanteissa, joissa käyttäjällä ei ole käyttäjätunnusta kohteessa, olipa kyseessä NT-toimialue tai NT-työasema.

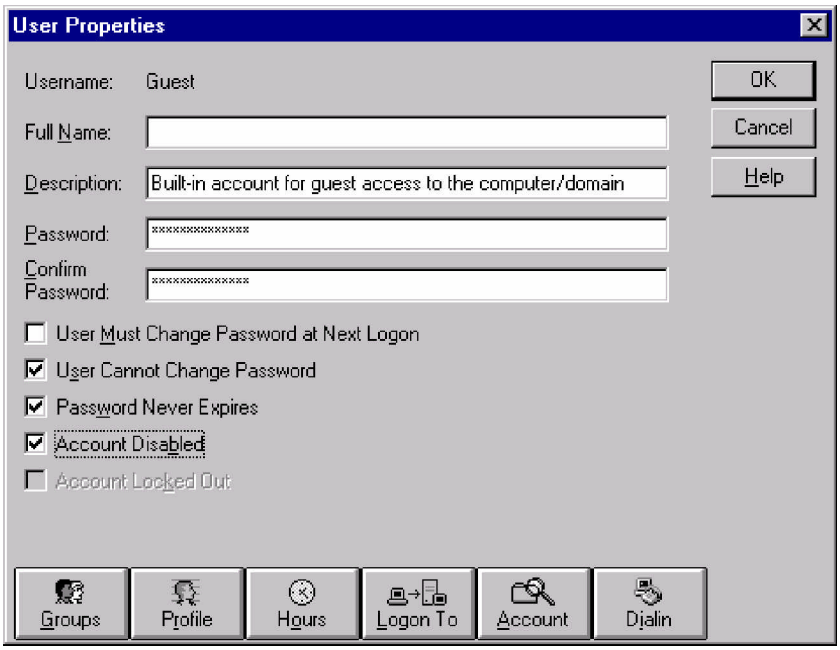
Guest-käyttäjätunnus ei vaadi salasanaa ja sitä voidaan käyttää paikalliseen kirjautumiseen tai kirjautumiseen verkon kautta. Nämä molemmat voidaan estää tai sallia: Guest-tunnuksen asetukset toimivat samoin kuin minkä tahansa NT:n käyttäjätunnuksen. Oletuksena Guest-käyttäjätunnus kuuluu Guest-ryhmään, jolla on oikeus kirjautua paikallisesti (**Log on locally**-oikeus).

Guest-tunnus voidaan kytkeä pois käytöstä (*Disabled*). Huomaa, että jos Guest-tunnus on käytössä, niin sekin kuuluu **Everyone** (Kaikki)-ryhmään.

Jos Guest-tunnus on käytettävissä, niin toimialueelle kirjautumaton käyttäjä *saattaa* saada automaattisesti käyttöönsä **Everyone** (Kaikki)-ryhmälle annettuja resursseja!

Suosituksia:

- Estä **Guest**-tunnuksen käyttö, tai jos haluat pitää sen käytössä, tarkista, mihin toimintoihin sen käyttö oikeuttaa. Tarkista tunnuksen asetukset paitsi toimialueilla, myös Windows NT-työasemissa!



- Tarkista User Manager for Domainsilla **Policies** | **User Rights** -asetukset: poista **Log on locally** -oikeus Guests-ryhmältä

- Poista tarvittaessa **Access this computer from network**-oikeus Guests-ryhmältä

- Testaa huolellisesti, mitä seuraa, jos poistat **Everyone**-ryhmältä oikeuden **Access this computer from network**.

Everyone

Everyone (Kaikki) on NT:ssä sisäänrakennettu kaikkien käyttäjien ryhmä, olivatpa nämä kirjautuneet NT-toimialueelle, NT-työasemaan tai **eivät**. Tämä saattaa tarjota tunkeutujille mukavan takaoven.

NT sisältää oletuksena paljon **Everyone**-ryhmälle annettuja oikeuksia. Niinpä siitä eroon pääseminen ei ole yksinkertainen asia, vaan käytännössä täysin mahdotonta. Suojauksia voidaan kuitenkin tehostaa tarvittaessa seuraavilla menettelyillä, esimerkiksi poistamalla **Everyone**-ryhmän oikeuksia mahdollisuuksien mukaan.

Olepa todella varovainen tässä operaatiossa!

Kirjaa kaikki tekemäsi toimenpiteet!

Kokeile seuraavaa:

- Luo **User Manager for Domainsilla** uusi ryhmä, vaikkapa **Every User** ja lisää siihen **kaikki** itse määritellyt käyttäjät (ei kuitenkaan Guest-käyttäjätunnusta)
- Anna tälle ryhmälle **Policies** | **User Rights** -asetuksissa **Access this computer from network** -oikeus
- Poista **Everyone**-ryhmältä **Access this computer from network** -oikeus
- Vaihda samoin kaikki muutkin oikeudet (anna oikeus **Every User**-ryhmälle ja poista oikeus **Everyone**-ryhmältä)
- Muuta oikeudet myös hakemistojen ja tiedostojen oikeuksissa; anna oikeus **Every User**-ryhmälle ja poista oikeus **Everyone**-ryhmältä (älä kuitenkaan tee tätä helpolla tavalla muuttamalla oikeudet suoraan koko hakemistopuulle)
- Muuta oikeudet samoin myös jaetuissa resursseissa: anna oikeus **Every User**-ryhmälle ja poista oikeus **Everyone**-ryhmältä
- Lopuksi jää jäljelle rekisteri, jossa oikeuksien muuttaminen saattaa olla mahdotonta. Helpointa lienee poistaa oikeudet **Everyone**-ryhmältä **HKEY_LOCAL_MACHINE**ssa ja antaa

tilalle antaa lukuoikeus **Every User**-ryhmälle.

Voit myös noutaa NT Securityn **Red Button**-työkalun, joka demonstroi näitä ongelmia, **http://www.NTSecurity.com**.

Microsoftin hotfix tähän löytyy osoitteesta:
ftp://ftp.microsoft.com/bussys/
winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP2/sec-fix/

Verkon kautta voit protokollatasolla rajoittaa pääsyä NT-koneisiin esimerkiksi kieltämällä porttien **UDP 137**, **UDP 138** ja **TCP 139** käytön. Voit myös käyttää useampia verkkokortteja ja sopivasti poistaa sidokset NetBEUI- ja TCP/IP-protokollilta sekä NetBIOS-rajapinnan. NT-työasemissa voidaan sulkea **SERVER**-palvelu.

Näissä, kuten muissakin suojausongelmissa, tärkeintä on **maltti** sekä **todellisten ongelmien suuruusluokan arviointi**. Lisäksi NT:n tuntemus auttaa asettamaan internetissä roihuavat NT Security Flaw -keskustelut oikeaan kategoriaan.

Hakemistot ja tiedostojärjestelmät

- Käytä **vain NTFS-tiedostojärjestelmää**. Siinä on edistyneet tietoturvaominaisuudet, joiden avulla voidaan estää tiedostojen luvaton käyttö

- Älä käytä NT-palvelimissa FAT-tiedostojärjestelmää kuin erityisistä syistä (esim. jos testaat uusia **Service Packeja** yhdessä palvelimessa, ja jos esimerkiksi NT:n ydin- tai käynnistystiedostot korruptoituvat - kuten monille kävi **Service Pack 2**:n tapauksessa)

- Windows NT voidaan käynnistää levykkeeltä Linux- tai **NTFSDOS.EXE**-käynnistyslevykkeellä, jolloin NTFS-suojaukset pystytään ehkä kiertämään (Windows 95:lle on myös NTFS-ohjain). Lukitse tai estä levykeaseman käyttö, tai poista tarvittaessa levykeasema. Sijoita palvelimet vain lukittuun tilaan

- Tiedota käyttäjille tiedostoihin liittyvistä käyttöoikeuksista ja siitä, että oikeudet voivat hävitä, kun tiedostoja kopioidaan

- Älä anna riskikäyttäjille mahdollisuutta ajaa ohjelmia hakemistossa, jossa he voivat kopioida tiedostoja

- Älä koskaan kopioi luottamuksellisia tiedostoja hakemistoihin, joissa ei ole riittäviä turvallisuusmäärityksiä

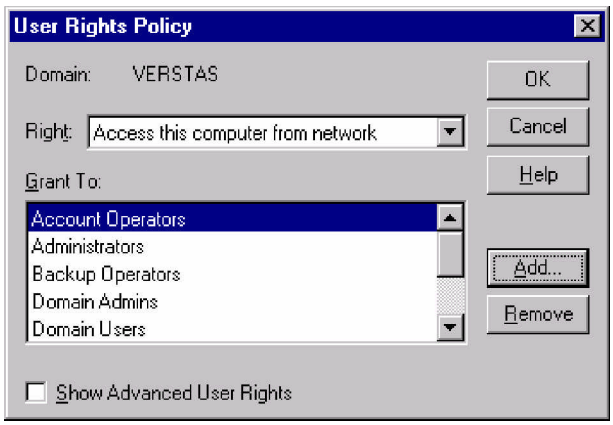
- Luo palvelimille järkeviä hakemistorakenteita, joiden avulla tiedostoja voidaan suojata - ei verkkoon jaettuja hakemistoja, joiden alihakemistoja on myös jaettu verkkoon!

- Jos tuotat tietoa julkiseen käyttöön, rajaa pääsy mahdollisuuksien mukaan vain tiettyihin hakemistoihin erillisillä palvelimilla.

Palvelimen ja työaseman käyttöoikeudet

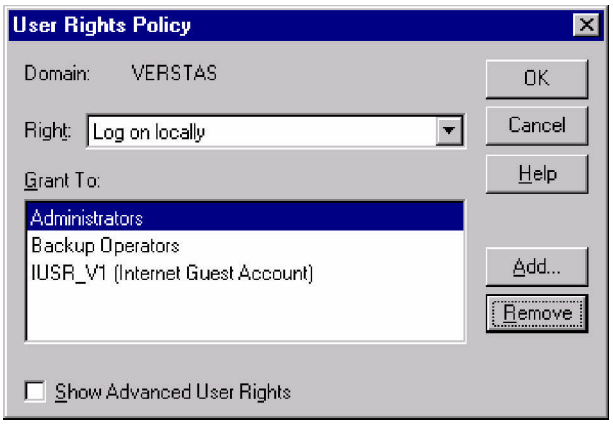
Voit rajoittaa sekä NT-palvelimen että -työaseman käyttöä seuraavilla menetelmillä:

- Voit rajoittaa palvelimen käyttöä verkon kautta **User Manager for Domainsilla** valitsemalla **Policies** | **User Rights** ja muuttamalla oikeuden **Access this computer from network** asetuksia. Oikeus on oletuksena mm. **Everyonella** (Kaikki); poistamalla tämän ryhmän ja määrittelemällä ryhmät erikseen voit rajata esimerkiksi palvelimen käyttöä verkon kautta.

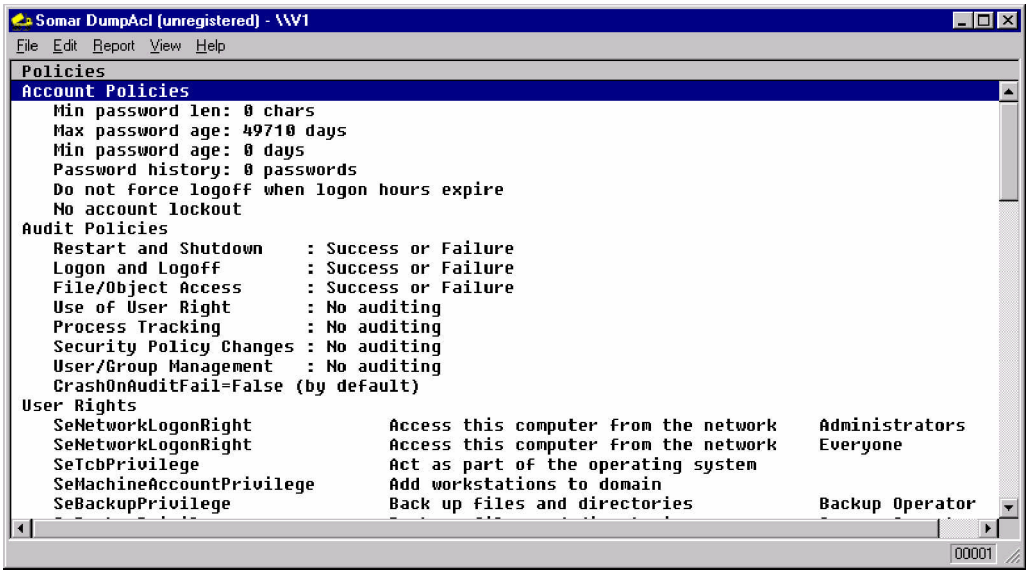


- Voit rajoittaa palvelimen paikallista käyttöä **User Manager for Domainsilla** valitsemalla **Policies** | **User Rights** ja muuttamalla oikeuden **Logon locally** asetuksia. NT-työasemassa oikeus on oletuksena mm. työaseman paikallisella **Users-ryhmällä.**

Poistamalla tarpeettomat ryhmät ja määrittelemällä ryhmät tai käyttäjätunnukset erikseen voit rajata paikalliset kirjautumisoikeudet vain rajatuille käyttäjäryhmille.



- **SomarSoftin**(**http://www.somar.com**) **DumpACL**-ohjelmalla voit kätevästi listata käyttöoikeudet.



NT-koneen piilottaminen

Windows NT -koneen piilottaminen tarkoittaa vain sitä, että kyseinen työasema tai palvelin ei lähetä selauspalvelun yleissanomia (*Broadcast*).

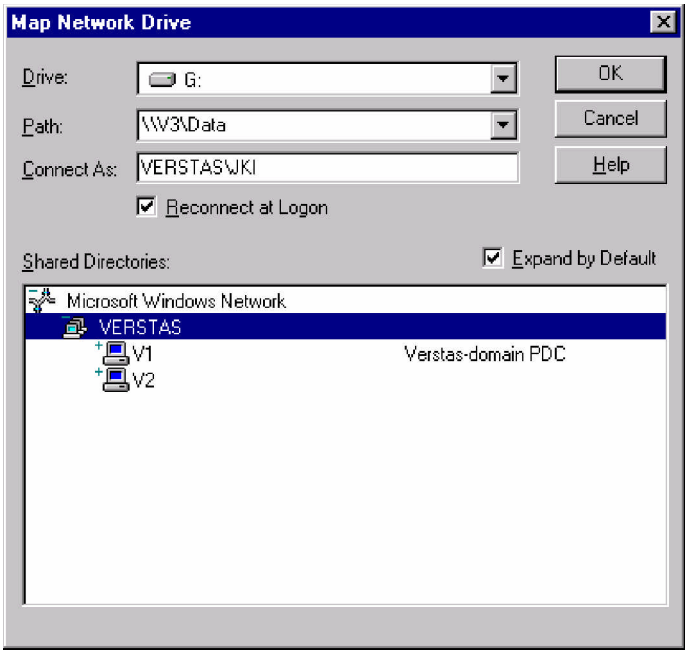
Suojauksiin se ei siis sinällään vaikuta, mutta kyseistä tietokonetta ei voi selailla verkosta esimerkiksi **File Managerilla** (Tiedostonhallinta) tai **Network Neighborhoodilla** (Verkkoympäristö).

Komentorivin komento on sekä NT-palvelimessa että -työasemassa

NET CONFIG SERVER /Hidden:Yes.

Koska tietokone ja sen jakamat resurssit eivät näy verkossa, niihin on viitattava UNC-nimillä, esimerkiksi **\\SERVERI\CDROM**.

Resurssien käyttöönotto tehdään kytkemällä levyasema **Map Network Drive** (Explorerissa **Tools** | **Map Network Drive**). Anna polku kohtaan **Path** ja tarvittaessa toinen käyttäjätunnus **Connect As**-valinnalla.



Toinen tapa on komentorivin komento

NET USE [levyasematunnus] /USER:toimialue\käyttäjä

Resurssin piilottaminen

Voit piilottaa jaetun resurssin antamalla resurssin viimeisenä merkkinä $-merkin. Huomaa, että NT:ssä on myös piilotettuja **oletusjakoja**: **IPC$**, **ADMIN$**, **PRINT$** - älä poista näitä jakoja!

Lisäksi levyasemien juurihakemistot on jaettu pääkäyttäjille: **C$**, **D$** jne. - jälleen yksi syy lisää saattaa suojaukset kuntoon NTFS:n avulla!

Koska jaettu resurssi eivät näy verkossa, niihin on viitattava UNC-nimillä, esimerkiksi

NET USE X: \\SERVERI\CDROM$.

Jaon voi lopettaa komentorivin komennolla

NET SHARE [jakonimi] /DELETE.

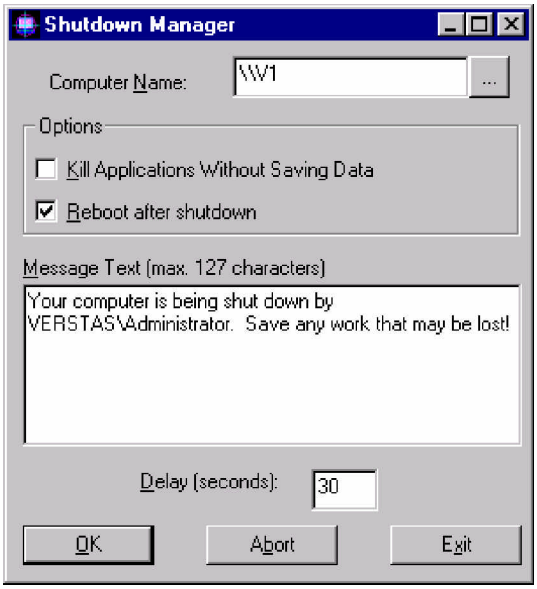
LogonPrompt

Myös Welcome-ikkunan teksti voidaan määritellä. Se tehdään lisäämällä nimi **LogonPrompt**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\EventLog\Application**
Nimi	**LogonPrompt**
Tyyppi	**REG_SZ**
Arvo	**Haluttu merkkijono, maksimipituus 256 merkkiä**

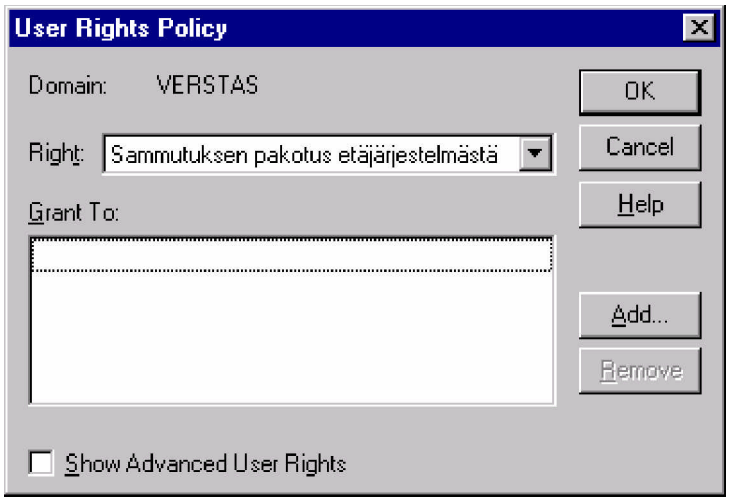
Shutdown

Resource Kitin **Shutdown Managerin** avulla voi sammuttaa (ja uudelleenkäynnistää) toisen NT-koneen. Se edellyttää **Järjestelmänvalvojan** (Administrator) oikeuksia tai **Server Operators** -ryhmän jäsenyyttä **kohdekoneessa**, ja aiemmissa NT-versioissa (ennen 4.0) tällä saattoi korkata kohdekoneen näytönsäästäjän!



Jos kohdekone on hyväksynyt alasajamisen, saat ilmoituksen:

Kyseessä on **User Manager for Domains:ssa** asetettava **Policy | User Rights** -oikeusasetus pakota sammutus etäjärjestelmästä **Force shutdown from a remote system**. Oletuksena oikeus on kohdekoneen Administrators- ja **Server Operators** -ryhmän jäsenillä. Poistamalla tämä oikeus ei etäkäynnistys ole mahdollinen.



Asetuksen voimaantulo edellyttää kohdekoneen uudelleenkäynnistystä. Tämän jälkeen etäkäynnistys ei toimi:

Automaattinen kirjautuminen

Vaikka Windows NT edellyttääkin aina käyttäjän kirjautumista järjestelmään, on myös mahdollista ottaa käyttöön automaattinen kirjautuminen annetulla oletuskäyttäjätunnuksella. Tällainen menettely voidaan ottaa käyttöön esimerkiksi luokkaympäristössä tai ns. Infokioskeissa. Se tosin romuttaa tehokkaasti käyttäjätunnuksiin liittyvän tietosuojan. Asetukset tulee tarvittaessa lisätä rekisteriin. Testaa ennen asetuksia, että pääset etähallitsemaan kyseisen NT-työaseman rekisteriä toisesta NT-koneesta!

Ensin kirjautumisen asetukset:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\Current Version\Winlogon**
Nimi	**AutoAdminLogon**
Tyyppi	**REG_SZ**
Arvo	**0** tai **1** (1 = automaattinen kirjautuminen voimassa)

Lisää käyttäjätunnus:

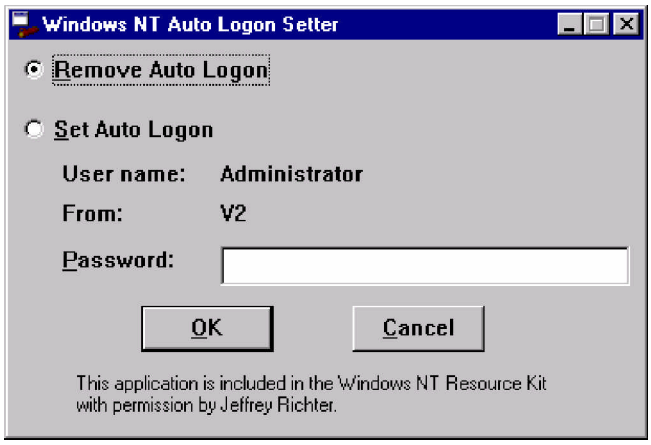
Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\Current Version\Winlogon**
Nimi	**DefaultUserName**
Tyyppi	**REG_SZ**
Arvo	Kirjautumisessa käytetty käyttäjätunnus

Lisää vielä salasana:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\Current Version\Winlogon**
Nimi	**DefaultPassword**
Tyyppi	**REG_SZ**
Arvo	Kirjautumisessa käytetty salasana

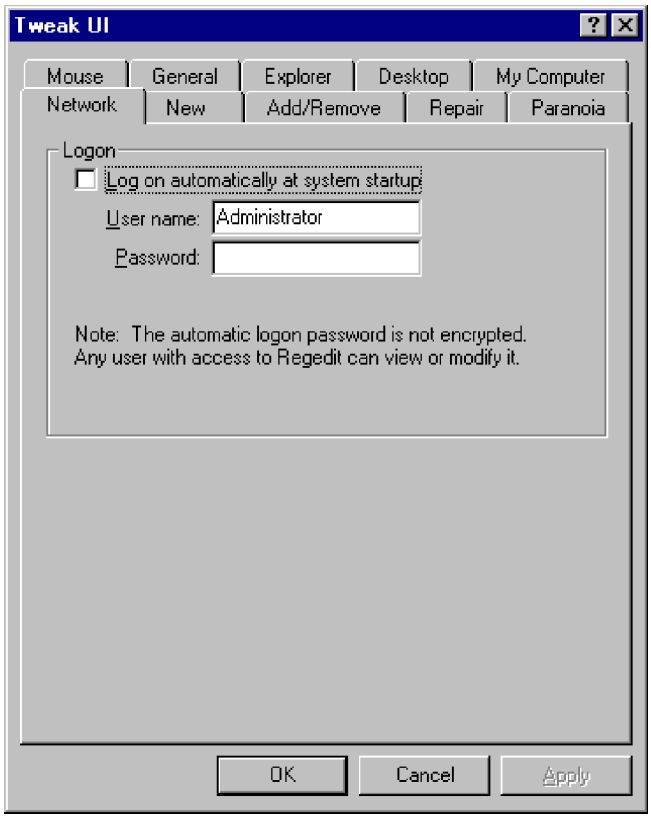
Tämä on määriteltävissä - myös poistettavissa - Resource Kitin **Auto Logon** -apuohjelmalla.

Älä missään tapauksessa määrittele pääkäyttäjän tunnuksilla automaattista kirjautumista!



Kirjautumisen voi ohittaa painamalla **vaihtonäppäintä** (Shift) kirjautumisvaiheessa.

Windows NT 4.0:n PowerToysin **TweakUI**:lla voi myös tehdä saman:

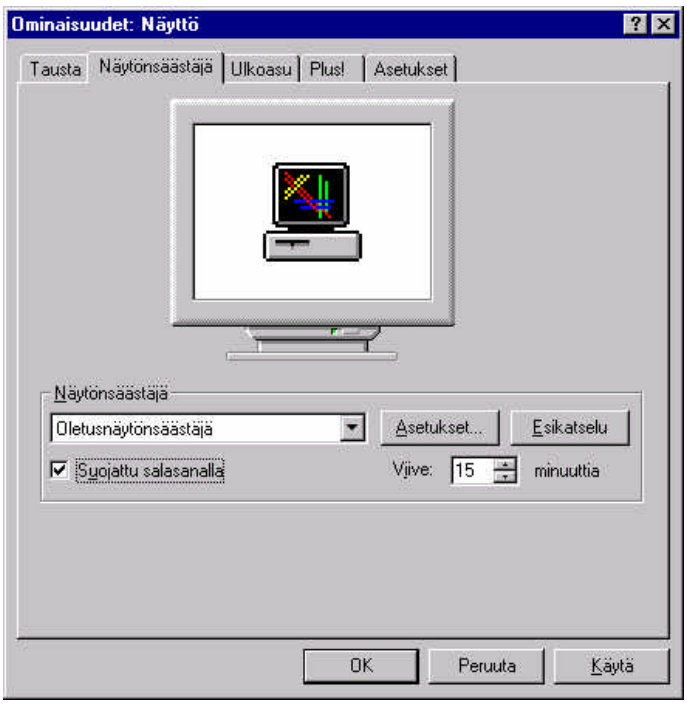


NT-koneen työaseman lukitseminen

Työaseman lukitseminen sekä NT-palvelimella että -työasemassa on syytä ottaa käyttöön, ainakin kirjauduttaessa pääkäyttäjien tunnuksilla.

Työaseman voi lukita painamalla **Ctrl+Alt+Del** ja **Enter** - oletuksena on **Lukitse työasema** (Lock Workstation). Työaseman voi lukita näytönsäästäjällä:

- 16-bittiset näytönsäästäjät eivät kuitenkaan takaa suojausta - NT:n 32-bittinen suojausalijärjestelmä ohittaa ne
- Suhtaudu skeptisesti muihin kuin NT:n mukana tuleviin näytönsäästäjiin
- Älä käytä palvelimissa 3D-näytönsäästäjiä - ne saattavat aiheuttaa tarpeetonta kuormitusta!



Event Viewerin suojaaminen

Voit suojata tapahtumalokin rekisteristä. Lisää nimi **RestrictGuestAccess** lokin kohdalle (**Application**, **Security** tai **System**), anna arvoksi **1** ja aseta nimeen oikeudet vain **Administrators**-ryhmälle and järjestelmälle **System**.

Esimerkiksi sovellusloki:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\EventLog\Application**
Nimi	**RestrictGuestAccess**
Tyyppi	**REG_SZ**
Arvo	**1**

Käynnistä lopuksi NT-kone uudelleen.

Kirjoitinohjainten asentamisen rajoittaminen

Voit rajoittaa kirjoitinohjainten lisäämisen **Administrators**- ja **Print operators** -ryhmälle tai **Power users** -ryhmälle.

Lisää **Servers**-avain ja lisää avaimen alle nimi **AddPrinterDrivers**. Anna arvoksi **1**.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Print\Providers\LanManPrintServices\Servers**
Nimi	**AddPrinterDrivers**
Tyyppi	**REG_SZ**
Arvo	**1**

Schedule-palvelun suojaaminen

AT-komennot ajetaan Schedule-palvelussa (ajoituspalvelu). Tavallisella käyttäjällä ei ole asiaa AT-komentoihin, mutta voit tarvittaessa sallia **Administrators-ryhmän** lisäksi oikeuden AT-komentoihin myös muille järjestelmäoperaattoreille.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\LSA**
Nimi	**SubmitControl**
Tyyppi	**REG_DWORD**
Arvo	**1**

Muille käyttäjille oikeutta ei voi antaa. Oikeus tulee voimaan uudelleenkäynnistyksessä.

Ongelmatilanteissa on hyvä muistaa, että tämäkin asetus on huonosti dokumentoitu, ja lisäksi sen toimintaan saattavat vaikuttaa muut asennetut palvelut.

Jos asetus toimii, muista päivittää **Emergency Repair Disk**!

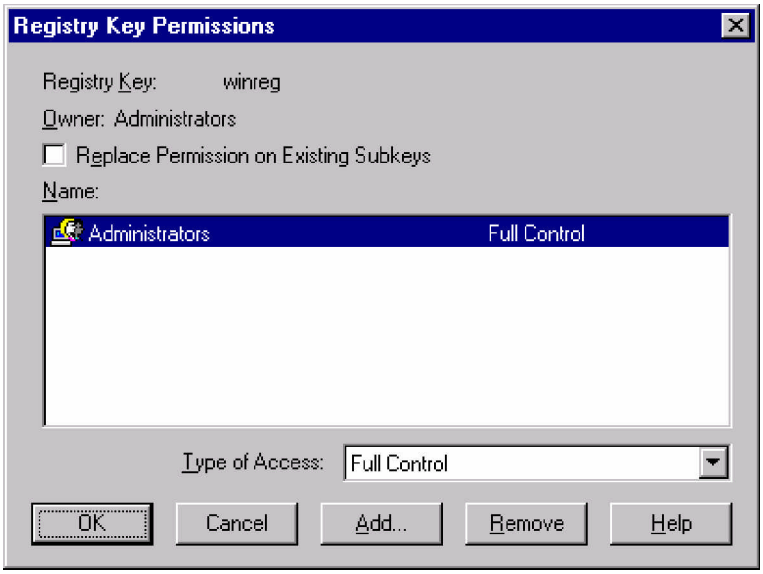
Rekisterin suojaaminen etäkäytöltä

Rekisterin etäkäyttöasetukset on määritelty rekisterissä avaimella **winreg**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentcontrolSet\Control\SecurePipeServers\winreg**
Nimi	
Tyyppi	
Arvo	Käyttäjien oikeudet winregiin määrittävät rekisterin etäkäyttöoikeudet

Oletuksena **winreg**-nimeä ei ole Windows NT -työasemassa (jolloin rekisterin etäkäyttö on rajoittamaton), mutta Windows NT -palvelimessa on. Palvelimessa sallitaan vain **Administrators-ryhmän** etäkäyttää rekisteriä.

Suojaukset voit asettaa **winreg**-avaimeen vain **REGEDT32.EXE**:llä käyttäen **Security** | **Permissions** -valintaa.



Jotkut palvelut, kuten monistuspalvelu **Directory Replicator** ja **Spooler** vaativat oikeuden rekisteriin. Voit joko lisätä oikeudet käyttäjätunnukselle (joka on määritelty palvelun käynnistykseen) tai sallia tiettyjen avainten käsittelyn **AllowedPaths** -avaimella. Nimet ovat **Machine** ja **Users**.

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentcontrolSet\Control\SecurePipeServers\winreg \AllowedPaths**
Nimi	**Machine**
Tyyppi	**REG_MULTI_SZ - Multi string**
Arvo	Sallitaan pääsy rekisterin polkuihin, oletukset: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Services\Replicator

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentcontrolSet\Control\SecurePipeServers\winreg \AllowedPaths**
Nimi	**Users**
Tyyppi	**REG_MULTI_SZ - Multi string**
Arvo	Sallitaan käyttäjille pääsy rekisterin polkuihin, oletus on tyhjä

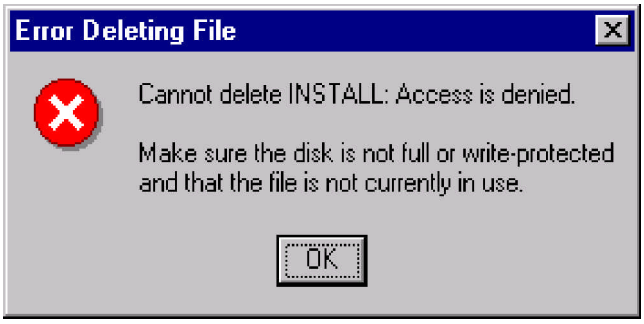
Käyttöoikeudet

Käyttäjän käyttöoikeudet johonkin tiettyyn tiedostoon muodostuvat yhdistelmänä sekä paikallisista kansion käyttöoikeuksista **Directory Permissions** että käyttöoikeuksista jaetuille resursseille **Access Through Share Permissions** annettavista käyttöoikeuksista.

Kansion käyttöoikeudet **Directory Permissions** määrittävät, mitä käyttäjät voivat tehdä kansiossa. Voit muuttaa kansion käyttöoikeuksia valitsemalla ensin kansion ja sitten hiiren pikavalikosta **Properties** | **Security** | **Permissions**. Oletuksena hakemiston käyttöoikeuksien määrittäminen koskee myös kaikkia hakemiston tiedostoja; erikseen voidaan asettaa oikeuksia myös tiedostokohtaisesti.

Käyttöoikeudet jaetuille resursseille **Access Through Share Permissions** määritellään valitsemalla kansion pikakuvakkeen **Sharing** tai kansion ominaisuuksista **Sharing**-välilehti.

Tässä esimerkissä tiedoston poistaminen ei ole sallittu:



Kansion käyttöoikeudet

Kansion käyttöoikeudet:

- Ainoastaan kansion käyttöoikeudet **Directory Permissions** ovat voimassa, jos käyttäjä on kirjoittautunut NT:hen paikallisesti, eli hän **ei** käytä työaseman/palvelimen jakamia hakemistoja verkon kautta. Kansion käyttöoikeudet voidaan määritellä vain, jos kyseinen levyasema käyttää **NTFS-tiedostojärjestelmää**.

- Käyttöoikeudet kumuloituvat; jos käyttäjällä on eri ryhmien kautta erilaiset oikeudet, hän saa niistä **kumuloituvat maksimioikeudet**. Kuitenkin ei käyttöoikeutta **No Access** ohittaa kaikki muut oikeudet!

- Pienin mahdollinen käyttöoikeus on luetteluoikeus **List (RX)(No Specified)**, joka on oltava, jotta käyttäjä näkee hakemiston tiedostojen ja alihakemistojen nimet. Jos käyttäjällä ei ole vähintään tätä oikeutta, hän ei voi siirtyä hakemiston alihakemistoihin.

Kansion käyttöoikeuksia voidaan asettaa vain Windows NT -tiedostojärjestelmää (NTFS) käyttävien levyasemien hakemistojen ja tiedostojen suojaamiseen. Jos käytössä on CD-ROM:in **CDFS**-, MS-DOS:in **FAT**- tai OS/2:n **HPFS**-tiedostojärjestelmä, suojauksia ei voi asettaa; tällöin käytössä ei ole **Security**-välilehteä tai -valikkoa.

Levykeasemaan tai levykkeelle ei voi asentaa muuta kuin FAT-tiedostojärjestelmän ja CD-ROM-asema käyttää CDFS-tiedostojärjestelmää; kumpaankaan ei voi asettaa kansion käyttöoikeuksia. **FAT**- tai **HPFS**-tiedostojärjestelmän voi kuitenkin tarvittaessa muuntaa NTFS-tiedostojärjestelmäksi komentorivin **CONVERT**-komennolla.

Kansion käyttöoikeuksien muuttaminen **ei muuta olemassa olevien alihakemistojen** ja **niiden tiedostojen käyttöoikeuksia**, ellei tätä erityisesti haluta, tulee valita alikansioiden oikeuksien korvaaminen **Replace Permissions on Subdirectories**. Luodessasi uusia tiedostoja tai alihakemistoja, ne perivät kansion käyttöoikeudet. Oikeudet ovat seuraavat:

- Luettelu - **List (RX)(No Specified)**

- Luku - **Read (RX)(RX)**

- Lisäys,ei määritetty - **Add (WX)(No Specified)**

- Lisäys ja luku - **Add and Read (RWX)(RX)**

- Muutos - **Change (RWXD)(RWXD)**

- Täydet oikeudet - **Full Control (All)(All)**

- Ei käyttöoikeutta - **No Access (None)(None)**

Oikeudet kumuloituvat siten, että ei käyttöoikeutta **No Access** kuitenkin ohittaa kaiken muun. Tätä voi käyttää, jos resurssiin on pääsy usealla eri käyttäjäryhmällä (jotka sisältävät samoja jäsenia) ja jos erityisesti halutaan tietyltä käyttäjältä tai käyttäjäryhmältä estää pääsy resurssiin.

Jos annat kaikille käyttäjille eli **Everyone**-ryhmälle käyttöoikeuden **No Access**, kukaan ei saa kansiota käyttöönsä, koska kaikki käyttäjät kuuluvat **Everyone**-ryhmään ja **No Access** ohittaa kaikki muut oikeudet!

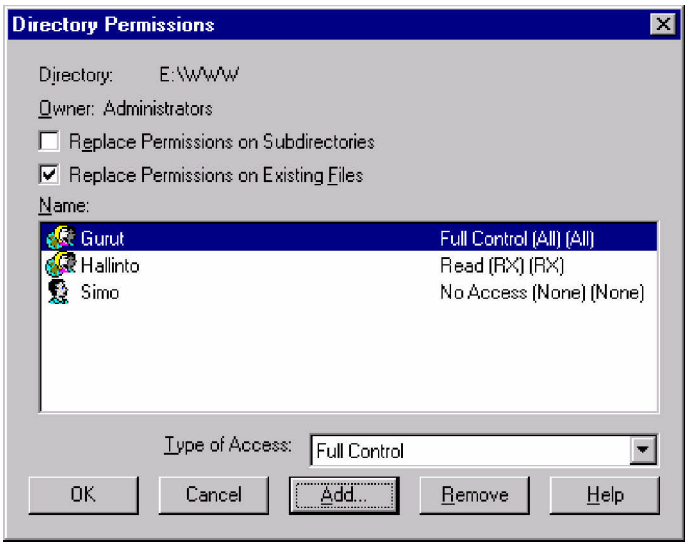
Kansioon vakiokäyttöoikeuden perässä näkyy kaksi lisämääritystä: ensimmäinen on kansion **käyttöoikeus** ja toinen on kansion **tiedostojen käyttöoikeus**.

Esimerkiksi eräät käyttöoikeudet ja ryhmäjäsenyydet taulukkona:

Oikeus	**Ryhmä**	**Ilpo**	**Jorma**	**Repe**	**Simo**
Read	Hallinto	**R**	**R**		
Full Control	Gurut	**R**		**R**	**R**
No Access					**K**

Gurut = Ilpo, Repe, Simo
Hallinto = Ilpo, Jorma
Oikeus ryhmäjäsenyyden kautta= R
Oikeus käyttäjätunnuksen kautta = K

Käyttöliittymässä:



- **Ilpo**, joka kuuluu sekä **Gurut**- että **Hallinto**-käyttäjäryhmiin; jos **Gurut**-käyttäjäryhmällä on tiettyyn kansioon täydet oikeudet **Full Control** ja **Hallinto**-käyttäjäryhmällä on vain lukuoikeus **Luku** (Read), Ilpolla on enemmän oikeuksia eli käyttöoikeus **Full Control** ryhmänsä **Gurut** kautta

- **Jorma** kuuluu **Hallinto**-käyttäjäryhmään. **Hallinto**-käyttäjäryhmällä on kansioon vain lukuoikeus **Read**; koska Jorma ei kuulu mihinkään muuhunkaan ryhmään eikä hänelle ole annettu suoraan muitakaan oikeuksia a.o. hakemistoon, hänellä on vain **lukuoikeus**

- **Repe**, joka kuuluu **Gurut**-käyttäjäryhmään, saa ryhmänsä kautta täydet oikeudet **Full Control**

- **Simolle**, joka kuuluu myös **Gurut**-käyttäjäryhmään, on suoraan asetettu ei käyttöoikeutta **No Access** - tämä ohittaa muut asetukset (Full Control), joten hänellä **ei ole mitään oikeuksia a.o. kansioon**.

Oikeudet ovat siis seuraavat:

Käyttäjä	Voimassa olevat käyttöoikeudet
Ilpo	Täydet oikeudet - Full Access
Jorma	Luku - Read

Repe	Täydet oikeudet - Full Access
Simo	Ei käyttöoikeutta - No Access

Vaikka käyttäjäryhmillä tai käyttäjillä on kansioon täydet oikeudet **Full Control**, he eivät voi poistaa kansion tiedostoja, jos **tiedostojen käyttöoikeudet** estävät sen.

Voit muuttaa kansion käyttöoikeuksia vain, jos olet kansion **omistaja** (Owner) tai sinulla on kansion omistajan antama **lupa** muuttaa käyttöoikeuksia.

Kun asetat kansioon vakiokäyttöoikeuden, sen perässä näkyy kaksi lisämääritystä: ensimmäinen on kansion **käyttöoikeus** ja toinen on kansion **tiedostojen käyttöoikeus**. Jos määrität kansioon esimerkiksi käyttöoikeuden lisäys & luku **Add & Read**, kansion vieressä näkyvät kirjaimet (**RWX**), jotka tarkoittavat käyttöoikeuksia **luku**, **kirjoitus** ja **suoritus** (Execute). Kansion tiedostojen vieressä näkyvät kirjaimet (**RX**), jotka tarkoittavat tiedostoihin kohdistuvia käyttöoikeuksia **luku** ja **suoritus**.

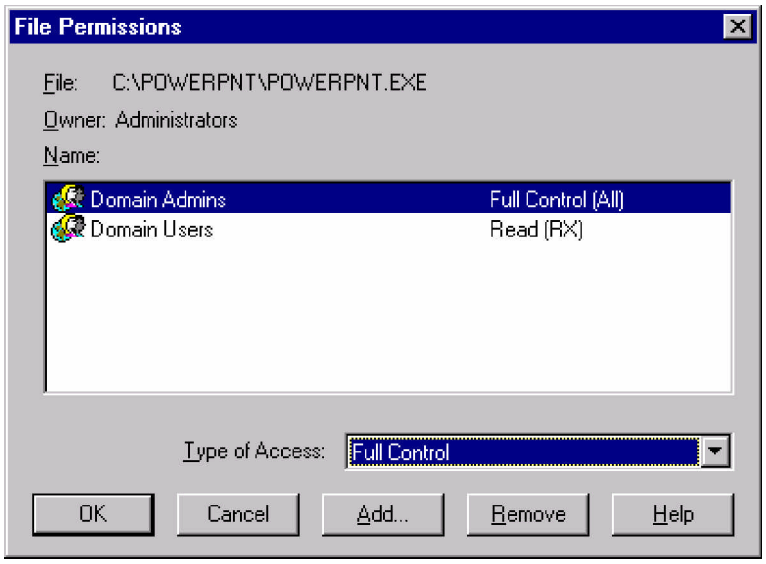
Jotkin hakemiston käyttöoikeudet määrittävät tiedoston käyttöoikeudeksi ei määritetyn **Not Specified**. Jos käyttäjälle tai ryhmälle ei ole määritetty tiedostojen käyttöoikeutta, kyseinen ryhmä tai käyttäjä **ei voi käyttää** kansion tiedostoja, ennen kuin käyttöoikeus määritetään jollakin muulla tavalla - yksi tapa on antaa käyttöoikeus yksittäisiin tiedostoihin. Useimmiten kannattaa pyrkiä antamaan oikeudet kuitenkin vain kansioiden kautta, poikkeuksena esimerkiksi tilanne jossa esimerkiksi sovelluksen asennusohjelman **SETUP.EXE** käyttö halutaan kieltää.

Joissakin tapauksissa ryhmällä tai käyttäjällä olevat hakemiston käyttöoikeudet eivät periydy alihakemistoille - tällaiset käyttöoikeudet merkitään tähdellä, esimerkiksi **(All)***.

Tiedostojen käyttöoikeudet

Tiedoston käyttöoikeudet määrittävät, mitä käyttäjät voivat tehdä saatuaan tiedoston käsittelyyn. Kun luot hakemistoon uusia tiedostoja, ne perivät hakemiston käyttöoikeudet. Tässäkin käyttöoikeudet täydentävät toisiaan; poikkeuksena on ei käyttöoikeutta **No Access**, joka kumoaa

kaikki muut käyttöoikeudet.



Voit muuttaa tiedoston käyttöoikeuksia vain, jos olet **tiedoston omistaja** tai sinulla on tiedoston omistajan antama lupa muuttaa käyttöoikeuksia.

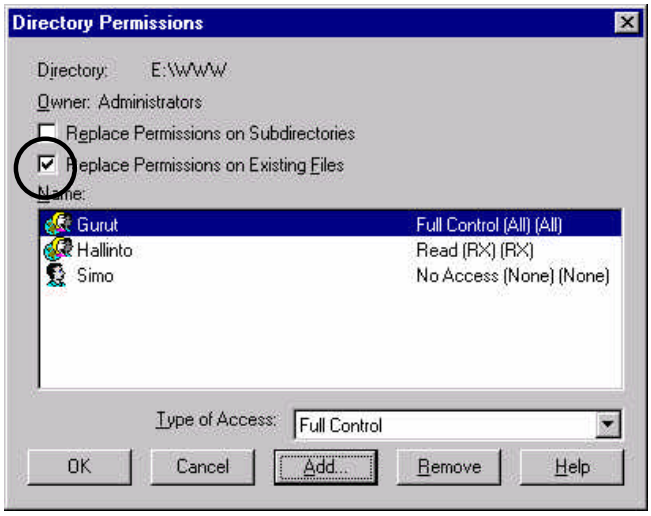
Yleensä vakiokäyttöoikeudet riittävät tiedostojen suojaamiseen. Jos kuitenkin tarvitset erityisesti asetettuja käyttöoikeuksia, käytä erityiskäyttöoikeuksia **Special Access**. Voit määrittää erityiskäyttöoikeudet hakemistoille, kaikille valittujen hakemistojen tiedostoille tai vain valituille tiedostoille. Jos määrität erityiskäyttöoikeudet kansiolle, käyttöoikeudet vaikuttavat vain kyseiseen kansioon, ei sen sisältämiin tiedostoihin.

Tiedoston käyttöoikeudet voivat olla seuraavat:

- Ei käyttöoikeutta - **No Access (None)**
- Luku - **Read (RX)**
- Muutos - **Change (RWXD)**
- Täydet oikeudet - **Full Control (All)**
- Erityisoikeudet - **Special Access (RWXDPO)**.

Yleensä neljä ensimmäistä vakiokäyttöoikeutta riittää tiedostojen suojaamiseen. Jos kuitenkin tarvitset erityisesti asetettuja käyttöoikeuksia, käytä erityisoikeuksia **Special Access**. Voit määrittää erityiskäyttöoikeudet kaikille tiedostoille tai vain valituille tiedostoille.

Kun määrität käyttöoikeudet **hakemistolle**, käyttöoikeudet **oletuksena** vaikuttavat myös kyseisen hakemiston tiedostoihin!

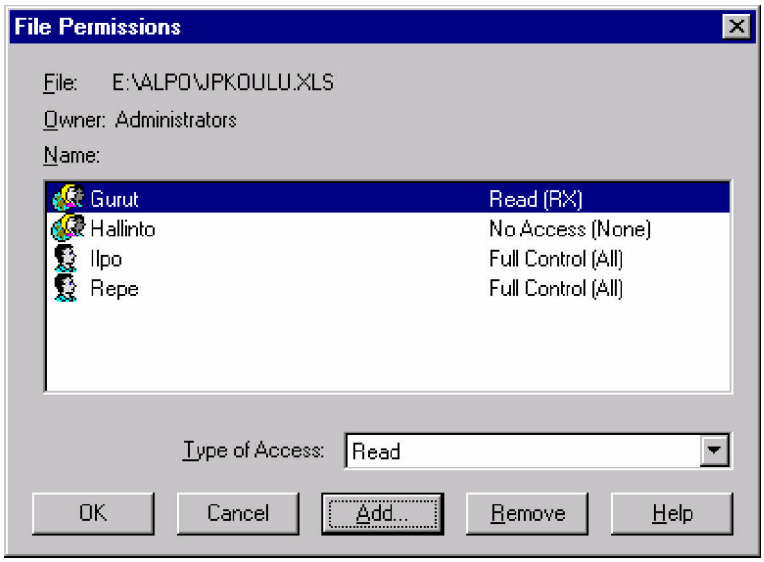


Esimerkiksi eräät tiedoston käyttöoikeudet ja ryhmäjäsenyydet taulukkona:

Oikeus	**Ryhmä**	**Ilpo**	**Jorma**	**Repe**	**Simo**
No Access	Hallinto	**R**	**R**		
Read	Gurut	**R**		**R**	**R**
Full Control		**K**		**K**	

Gurut = Ilpo, Repe, Simo
Hallinto = Ilpo, Jorma
Oikeus ryhmäjäsenyyden kautta= R
Oikeus käyttäjätunnuksen kautta = K

Käyttöliittymässä:



- **Ilpo**, joka kuuluu sekä **Gurut**- että **Hallinto**-käyttäjäryhmiin saa periaatteessa käyttäjätunnuksensa kautta tiedostoon jopa täydet oikeudet **Full Control** (ja **Gurut**-ryhmän kautta lukuoikeuden **Read**), mutta koska **Hallinto**-käyttäjäryhmällä on tiedostoon asetettu **No Access**, se ohittaa muut asetukset, joten **Ilpolla ei ole oikeuksia tiedostoon**

- **Jorma** kuuluu **Hallinto**-käyttäjäryhmään. **Hallinto**-käyttäjäryhmällä ei ole tiedostoon käyttöoikeutta **No Access** - tämä ohittaa muut asetukset (Full Control), joten hänellä **ei ole mitään oikeuksia tiedostoon**

- **Repe**, joka kuuluu **Gurut**-käyttäjäryhmään, saa ryhmänsä kautta vain lukuoikeuden **Read**; mutta suoraan käyttäjätunnuksensa kautta tiedostoon täydet oikeudet **Full Control**

- **Simo** saa **Gurut**-käyttäjäryhmänsä kautta vain lukuoikeuden **Read**.

Oikeudet ovat siis seuraavat:

Käyttäjä	Voimassa olevat käyttöoikeudet
Ilpo	Ei käyttöoikeutta - No Access
Jorma	Ei käyttöoikeutta - No Access
Repe	Täydet oikeudet - Full Control
Simo	Lukuoikeus - Read

Jaetun kansion käyttöoikeudet

Käyttöoikeudet voi määrittää jaetun kansion avulla riippumatta siitä, onko hakemisto Windows NT -tiedostojärjestelmää (NTFS), FAT-tiedostojärjestelmää vai HPFS-tiedostojärjestelmää käyttävässä asemassa.

Seuraavien sääntöjen noudattaminen tehostaa jaettujen hakemistojen suojaamista:

- Jaetun kansion kautta määritetyt käyttöoikeudet ovat voimassa vain silloin kun tiedostoa käsitellään verkon yli, olipa kyseessä FAT- tai NTFS-tiedostojärjestelmää käyttävä kiintolevy

- Jaetun kansioon kautta määritetyt käyttöoikeudet vaikuttavat **kaikkiin** jaetun kansioon tiedostoihin ja alihakemistoihin

- NTFS-tiedostojärjestelmää käyttävän kiintolevyn kansioon käyttöoikeuksiin verkon yli vaikuttavat sekä paikalliset kansion käyttöoikeudet että jaetun kansion kautta määritetyt käyttöoikeudet

- Jaetulle kansiolle määritetyt paikalliset käyttöoikeudet ratkaisevat, kuinka laajat käyttöoikeudet käyttäjällä voi paikallisesti enimmillään olla. Tämä tietysti pätee, vaikka kansiota ei olisikaan jaettu

- Jos käyttäjä käyttää kansiota verkon kautta ja hänellä on eri ryhmien kautta erilaiset oikeudet, hän saa niistä kumuloituvat maksimioikeudet

- Käyttäjän käyttöoikeudet johonkin tiettyyn tiedostoon muodostuvat yhdistelmänä sekä paikallisista kansion käyttöoikeuksista **Directory Permissions** että verkon kautta jaetuille resursseille **Access Through Share Permissions** annettavista käyttöoikeuksista

Yhteensä kuitenkaan e.m. oikeudet eivät kumuloidu, vaan käyttäjän voimassa olevat oikeudet ovat **minimioikeudet** sekä hakemiston käyttöoikeuksista että verkon kautta jaetulle resurssille annetuista käyttöoikeuksista.

Oletuksena NTFS-levyiltä jaetuissa hakemistoissa kaikilla käyttäjillä eli **Everyone**-ryhmällä on täydet oikeudet **Full Control**!

Voit määrittää seuraavat käyttöoikeudet jaetulle resurssille **Access Through Share Permissions**, pienimmästä suurimpaan:

- Luku - **Read**

- Muutos - **Change**

- Täydet oikeudet - **Full Control**

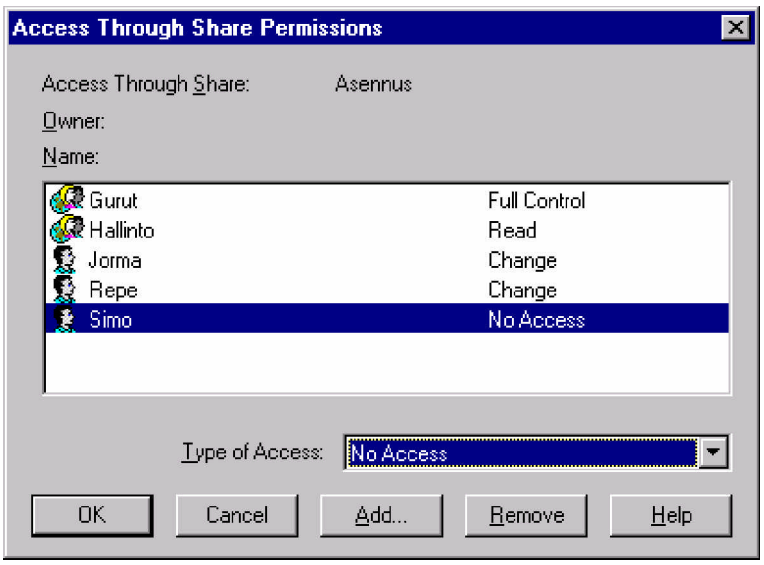
- Ei käyttöoikeutta - **No Access**.

Esimerkiksi erään jaetun hakemiston **Asennus** käyttöoikeudet ja ryhmäjäsenyydet verkon kautta taulukkona:

Oikeus	Ryhmä	Ilpo	Jorma	Repe	Simo
Read	Hallinto	**R**	**R**		
Change			**K**	**K**	
Full Control	Gurut	**R**		**R**	**R**
No Access					**K**

Gurut = Ilpo, Repe, Simo
Hallinto = Ilpo, Jorma
Oikeus ryhmäjäsenyyden kautta= R
Oikeus käyttäjätunnuksen kautta = K

Käyttöliittymässä:



Oikeudet ovat siis seuraavat:

- **Ilpo**, joka kuuluu sekä **Gurut**- että **Hallinto**-käyttäjäryhmiin; jos **Gurut**-käyttäjäryhmällä on täydet oikeudet **Full Control** verkon kautta ja **Hallinto**-käyttäjäryhmällä on vain lukuoikeus **Read**, on Ilpolla verkon kautta täydet oikeudet **Asennus**-jakoon

- **Jormalla** on Hallinto-ryhmän kautta lukuoikeus **Read**, mutta suoraan käyttäjäkohtaisesti muutosoikeus **Change**-oikeus; niinpä voimassa on suurempi eli **Change**-oikeus

- **Repe**, joka kuuluu **Gurut**-käyttäjäryhmään, saa ryhmän kautta täydet oikeudet **Full Control**, vaikka muuten hänellä olisi suoraan käyttäjäkohtaisesti vain muutosoikeus **Change**; niinpä voimassa on täydet oikeudet **Full Control**

- **Simolle**, joka kuuluu **Gurut**-käyttäjäryhmään, on estetty käyttö henkilökohtaisesti oikeudella **No Access**, mikä ohittaa muut oikeudet (**Full Control**) joten hänellä ei ole mitään oikeuksia a.o. hakemistoon verkon kautta. Paikallisella tasolla eli hakemistotasolla hänellä toki voi olla mitkä oikeudet tahansa; tällöin **Simon** on kirjoittauduttava palvelimeen tai työasemaan paikallisesti käyttäjäksi (Logon locally -oikeus!) voidakseen käyttää hakemiston tiedostoja. Verkon kautta hän ei voi käyttää tiedostoja.

Oikeudet verkon kautta ovat siis tässä tapauksessa seuraavat, riippumatta siitä onko kyseessä FAT-, NTFS- vai CDFS-levy:

Käyttäjä	Voimassa olevat oikeudet
Ilpo	Täydet oikeudet - Full Control
Jorma	Muutos - Change
Repe	Täydet oikeudet - Full Control
Simo	Ei käyttöoikeutta - No Access

Jaetun kansion käyttöoikeudet NTFS-levyllä

NTFS-levyllä kansion käyttöoikeuksiin verkon yli vaikuttavat sekä paikalliset kansion käyttöoikeudet että jaetun kansion kautta määritetyt käyttöoikeudet.

Käyttäjän tehokkaat oikeudet NTFS-levyn tiedostoon määräytyvät seuraavasti:

- Jaetulle kansiolle ja tiedostolle määritetyt **paikalliset käyttöoikeudet** ratkaisevat, kuinka laajat käyttöoikeudet käyttäjällä voi paikallisesti (ja ylipäätään) enimmillään olla. Nämä oikeudet pätevät, vaikka kansiota ei olisikaan jaettu. Oikeudet kumuloituvat, mutta **No Access** ohittaa kaikki muut oikeudet

- Jos käyttäjä käyttää kansiota verkon kautta ja hänellä on eri ryhmien kautta erilaiset oikeudet, hän saa niistä kumuloituvat maksimioikeudet. **No Access** ohittaa kaikki muut oikeudet

- Käyttäjän käyttöoikeudet johonkin tiettyyn tiedostoon muodostuvat yhdistelmänä sekä paikallisista kansion käyttöoikeuksista **Directory Permissions** että verkon kautta jaetuille resursseille **Access Through Share Permissions** annettavista käyttöoikeuksista. Yhteensä e.m. oikeudet eivät kumuloidu, vaan käyttäjän voimassa olevat oikeudet ovat **minimioikeudet** sekä hakemiston käyttöoikeuksista että verkon kautta jaetulle resurssille annetuista käyttöoikeuksista.

Oletuksena NTFS-levyiltä jaetuissa hakemistoissa kaikilla käyttäjillä eli **Everyone** -ryhmällä on täydet oikeudet **Full Control**!

Esimerkki: käyttöoikeudet jaetulle resurssille **Access Through Share Permissions**:

Oikeus	**Ryhmä**	**Ilpo**	**Jorma**	**Repe**	**Simo**
Read	Hallinto	**R**	**R**		
Full control	Gurut	**R**		**R**	**R**
No Access					**K**

Gurut = Ilpo, Repe, Simo
Hallinto = Ilpo, Jorma
Oikeus ryhmäjäsenyyden kautta= R
Oikeus käyttäjätunnuksen kautta = K

Käyttäjä	**Voimassa olevat oikeudet**
Ilpo	Täydet oikeudet - Full Control
Jorma	Luku - Read
Repe	Täydet oikeudet - Full Control
Simo	Ei käyttöoikeutta - No Access

Kansion käyttöoikeudet **Directory Permissions**:

Oikeus	**Ryhmä**	**Ilpo**	**Jorma**	**Repe**	**Simo**
List		**K**		**K**	
Read	Hallinto	**R**	**R**		
Change			**K**		
Full control	Gurut	**R**		**R**	**R**
No access				**K**	

Gurut = Ilpo, Repe, Simo
Hallinto = Ilpo, Jorma
Oikeus ryhmäjäsenyyden kautta= R
Oikeus käyttäjätunnuksen kautta = K

Käyttäjä	Voimassa olevat oikeudet
Ilpo	Täydet oikeudet - Full Control
Jorma	Muutos - Change
Repe	Ei käyttöoikeutta - No Access
Simo	Täydet oikeudet - Full Control

Huomioiden kansioiden oikeudet lopulliset oikeudet käytettäessä tiedostoja verkon kautta ovat kuitenkin seuraavat:

Käyttäjä	Voimassa olevat oikeudet verkon kautta
Ilpo	Täydet oikeudet - Full Control
Jorma	Luku - Read
Repe	Täydet oikeudet - Full Control
Simo	Ei käyttöoikeutta - No Access

Käyttäjä	Voimassa olevat oikeudet kansioon
Ilpo	Täydet oikeudet - Full Control
Jorma	Muutos - Change
Repe	Ei käyttöoikeutta - No Access
Simo	Täydet oikeudet - Full Control

Oikeudet kansioon verkon kautta saadaan etsimällä ensin oikeudet kansio/verkkotasolla ja sitten etsimällä pienimmät samanaikaisesti kansio/verkkotasolla voimassa olevat oikeudet:

Käyttäjä	Oikeudet kansioon verkon kautta
Ilpo	Täydet oikeudet - Full Control
Jorma	Luku - Read
Repe	Ei käyttöoikeutta - No Access
Simo	Ei käyttöoikeutta - No Access

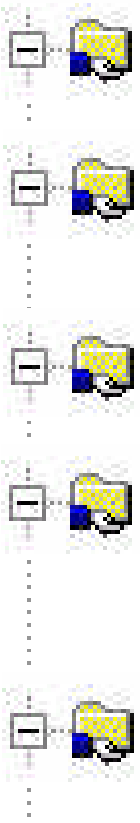
Kaksien eri oikeuksien määrittely johtaa helposti ongelmiin:

- Käyttäjällä ei ole riittävästi oikeuksia haluttuun resurssiin
- Käyttäjällä on liikaa oikeuksia haluttuun resurssiin
- Käyttäjällä on oikeuksia resurssiin, jonka käyttöön käyttäjällä ei tulisi olla ollenkaan oikeuksia.

Niinpä suosittelen seuraavan menetelmän harkitsemista:

- Jaa resurssit vain NTFS-levyiltä (varsinkin profiilihakemistot ja kotihakemistot)
- Jaa mahdollisimman harvoja hakemistoja verkkoon - älä jaa jaetun hakemiston alihakemistoja erikseen!
- Suunnittele tehokas hakemistorakenne ja käytä NTFS:n mahdollistamia kansio- ja tiedostotason suojauksia. Muista oikeuksien kumuloituminen! Vähimmäisoikeudet ovat luettelu **List**-oikeudet, jotka tulee olla, jotta käyttäjät voivat siirtyä jaetun hakemiston alihakemistoihin
- Lopuksi jaa hakemistoja verkkoon kaikille käyttäjille **Everyone** kaikilla oikeuksilla **Full Control**! Näin voit tehdä, jos suojaukset ovat kunnossa.

Tässä esimerkissä hakemistot on jaettu verkkoon omilla nimillään, ja oikeudet verkon kautta ovat **Everyone**-ryhmälle **Full Control**-oikeuksin.



\Data
\Budjetti
\Projekti

\Profiles
\Ilpo
\Repe
\Hallinto

\Apps
\WP
\Office

\Asennus
\Win95SF
\NT4\Wks\i386
\NT4\Srv\i386
\SP3US

\Users
\Ilpo
\Jorma
\Repe
\Simo

Hakemisto	Hakemiston kuvaus ja NTFS-oikeudet
Data	Käyttäjien datatiedostoja, päähakemistossa luetteluoikeus **List**, alihakemistoilla oikeudet asetettu käyttäjäryhmäkohtaisesti
Profiles	Profiilien hakemistot, päähakemistossa luetteluoikeus **List**, alihakemistoilla oikeudet asetettu joko lukuoikeus **Read** tai täydet oikeudet **Full Control** riippuen siitä, onko käyttäjällä pakollinen profiili vai ei. **Hallinto**-hakemisto on a.o. käyttäjäryhmän yhteinen profiili, ja hakemistoon on lukuoikeus **Read**
Apps	Sovellusten hakemistot, käyttäjillä lukuoikeus Read, järjestelmänvalvojilla oikeudet tarpeen mukaan
Asennus	Sovellusten asennushakemistot, vain järjestelmänvalvojilla **Full Control**
Users	Käyttäjien kotihakemistoja, päähakemistossa luetteluoikeus **List**, alihakemistoilla oikeudet asetettu **Full Control** käyttäjäkohtaisesti

Oletussuojaukset

Seuraavat ovat oletusoikeudet NT:n järjestelmälevyllä (esimerkissä **C:**) käytettäessä NTFS-tiedostojärjestelmää:

C:\	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%\msapps	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%\repair	Oikeudet
Everyone	Full Control

C:\%SystemRoot%\system	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%\system32	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%\config	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	List
System	Full Control

C:\%SystemRoot%\system32\dhcp	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\drivers	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\Ils	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%\system32\os2	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%\system32\ras	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change (rwxd)
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\repl	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read (rx)
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\repl\export	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

C:\%SystemRoot%\system32\repl\export\scripts	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Replicator	Change (rwxd)
Everyone	Read (rx)
Server Operators	Change (rwxd)
System	Full Control

C:\%SystemRoot%\system32\repl\import	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Replicator	Change (rwxd)
Everyone	Read (rx)
Server Operators	Change (rwxd)
System	Full Control

C:\%SystemRoot%\system32\spool	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Print Operators	Full Control
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\spool\drivers	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read (rx)
Print Operators	Full Control
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\spool\drivers\w32x86	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read (rx)
Print Operators	Full Control
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\spool\drivers\w32x86\2	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read (rx)
Print Operators	Full Control
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\spool\printers	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read (rx)
Print Operators	Full Control
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\spool\prtprocs	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read (rx)
Print Operators	Full Control
Server Operators	Full Control
System	Full Control

C:\%SystemRoot%\system32\spool\wins	Oikeudet
Everyone	Full Control

C:\temp	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

Muut hakemistot	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Change
Server Operators	Change
System	Full Control

CONVERT-komennolla NTFS:lle muunnetut levyt	Oikeudet
Everyone	Full Control

Käyttäjien hallintatyökalujen suojaukset

Windows NT -työaseman käyttäjätunnuksia hallitaan **Käyttäjien hallinnalla** (User Manager), jonka ohjelmatiedosto on **MUSRMGR.EXE**. Aseta tähän ja tarvittaessa muihinkin järjestelmä- ja ohjelmatiedostoihin tiukemmat suojaukset, esimerkiksi estä asetuksia muuttavien sovellusten käyttö tehokäyttäjiltä **Power users**.

Toimialueen käyttäjiä hallitaan User Manager for Domainsilla **USRMGR.EXE**. Voi asentaa Windows NT 4.0/Windows 95-työasemaan sen esim. Windows NT 4.0 Serverin CD-ROM:ilta tai Windows NT 4.0 -työasemaan myös **Resource Kitistä**.

Rekisterin suojaukset

Rekisteri sijaitsee oletuksena järjestelmälevyllä hakemistossa **WINNT\SYSTEM32\CONFIG**. FAT-levyllä ei ole mitään suojauksia; NTFS-levyllä oletuksena kaikilla käyttäjillä **Everyone** on luettelu **List**-oikeus. Suojaaminen voidaan tehdä esimerkiksi **C2 Configuration Managerilla**.

Poista rekisterieditorit **REGEDIT.EXE** ja **REGEDT32.EXE** työasemista.

Käynnistystiedostojen suojaukset

Käynnistystiedostoissa **C:\boot.ini**, **C:\ntdetect.com**, **C:\ntldr** voisi olla täydet oikeudet **Full Control** vain järjestelmänvalvojilla **Administrators** ja järjestelmällä **System**.

C:\boot.ini C:\ntdetect.com C:\ntldr	**Oikeudet**
Administrators	Full Control
System	Full Control

Samoin **C:\Autoexec.bat** ja **C:\Config.sys** voisi olla täydet oikeudet **Full Control** järjestelmänvalvojilla **Administrators** ja järjestelmällä **System**, kaikille käyttäjille **Everyone** voisi antaa lukuoikeuden **Read**.

C:\Autoexec.bat C:\Config.sys	**Oikeudet**
Administrators	Full Control
Everyone	Read
System	Full Control

Temp-hakemistoon voisi asettaa seuraavat oikeudet:

C:\temp	**Oikeudet**
Administrators	Full Control
Creator/owner	Full Control
Everyone	Add
System	Full Control

Järjestelmätiedostojen suojaukset

Windows NT:n asennuksen jälkeen voit muuttaa seuraaviin hakemistoihin annetut suojaukset, niin saat käyttöösi hieman tehokkaammat suojaukset.

C:\Winnt	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	Read
System	Full Control

C:\Wint\repair	Oikeudet
Administrators	Full Control

C:\Winnt\system32\config	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Everyone	List
System	Full Control

C:\Winnt\system32\spool	Oikeudet
Administrators	Full Control
Creator/owner	Full Control
Power Users	Change
System	Full Control

C:\Winnt\cookies **C:\Winnt\history** **C:\Winnt\profiles** **C:\Winnt\Temporary Internet Files**	**Oikeudet**
Administrators	Full Control
Creator/owner	Full Control
Everyone	Add
System	Full Control

Cacls

Cacls on Windows NT:n komento, joka näyttää hakemiston tai tiedoston käyttöoikeudet.

Esimerkiksi **DATA**-hakemiston käyttöoikeudet:

```
C:\>cacls data
C:\DATA Everyone:(OI)(IO)C
        Everyone:(CI)C
        BUILTIN\Administrators:(OI)(IO)F
        BUILTIN\Administrators:(CI)F
        CREATOR OWNER:(OI)(IO)F
        CREATOR OWNER:(CI)F
        NT AUTHORITY\SYSTEM:(OI)(IO)F
        NT AUTHORITY\SYSTEM:(CI)F
```

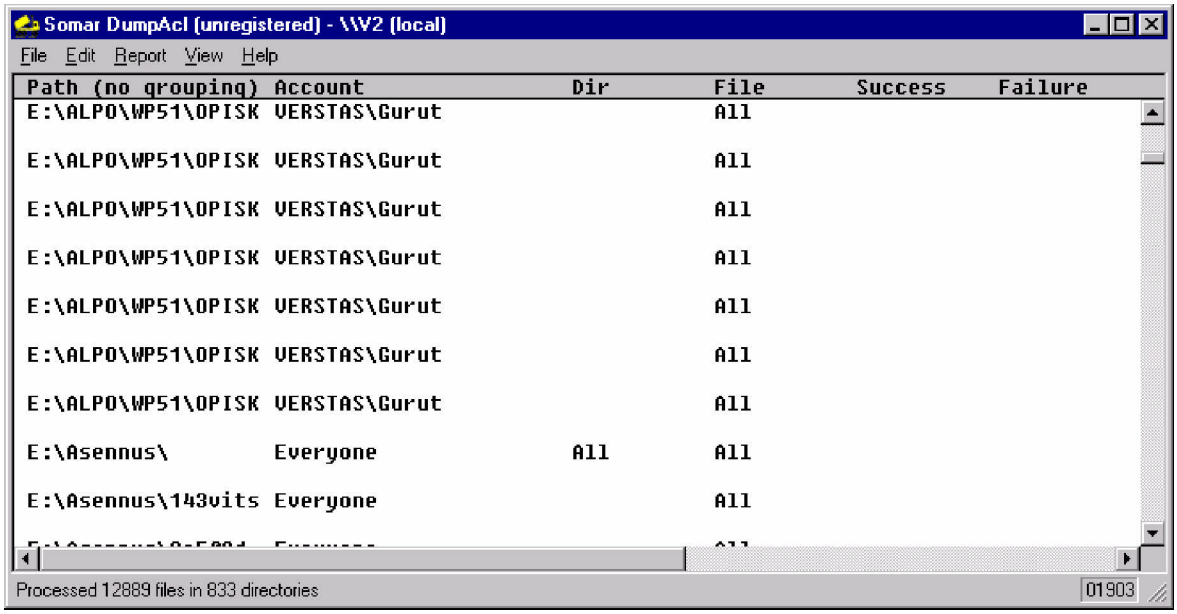
Tiedoston **INSTALL.LOG** oikeudet:

```
C:\DATA>cacls install.log
C:\DATA\INSTALL.LOG Everyone:C
                    BUILTIN\Administrators:F
                    CREATOR OWNER:F
                    NT AUTHORITY\SYSTEM:F
```

Käyttöoikeuksien hallintaan tulee myös Resource Kitin mukana joitakin apuohjelmia (**FIXACLS**, **PERMCOPY**, **PERMS**, **SCOPY**, **SUBINACL** ja **XCACLS**).

DumpACL

Työkalu, jolla voit listata tiedostojen ja kansioiden suojauksia kätevästi, löytyy **SomarSoftilta** (**http://www.somar.com**). SomarSoftin **DumpACL** on yksi helppokäyttöisimmistä ja luotettavimmista käyttöoikeuksien dumppausohjelmista.



Profiilien suojaaminen

Windows NT 4.0:ssa jokaisella käyttäjällä on **profiili**. Profiili voi olla:

- **Paikallinen** (Local)
- **Palvelimella**(Roaming)
- **Pakollinen** (Mandatory)

Voit suojata käyttäjän profiilin useammalla tavalla:

- Muutoksia vastaan määrittelemällä pakollisen profiilin sekä tallentamalla profiilin NTFS-levylle ja antamalla vain kyseiselle käyttäjälle oikeuksia kyseiseen hakemistoon
- Antamalla kyseiselle käyttäjälle vain lukuoikeudet kyseiseen hakemistoon proliifin luomisen jälkeen
- Määrittelemällä profiilin käyttöoikeudet vain kyseiselle käyttäjälle.

Käyttäjän profiili sisältää kaksi osaa:

1) Järjestelmäkansiot (*folder*), jotka sijaitsevat **Profiles**-järjestelmähakemistossa (**\%Systemroot%\Profiles**, esimerkiksi työasemassa **C:\Winnt\Profiles**). Alihakemistoista tärkeimpiä voi käsitellä tarvittaessa suoraan **Käynnistä** (Start)-valikosta

- **Desktop** (Työpöytä)-hakemistossa on käyttäjän työpöytä
- **Recent** -hakemistossa on pikakuvakkeet viimeksi käsitellyistä tiedostoista
- **SendTo** -hakemistossa on pikakuvakkeet hiiren pikavalikon **Lähetä** (Send)-valintaan
- **StartMenu** (Käynnistä-valikko) on käynnistysvalikon kansio.

Lisäksi on joitakin **piilotettuja** hakemistoja:

- **NetHood** -verkkoympäristö
- **PrintHood** - kirjoittimet
- **Templates** - mallit

2) Tiedosto **NTUser.dat** on käyttäjätunnuksen mukaisessa **Profiles**-järjestelmähakemiston alihakemistossa. Profiiliitiedostoon **NTUser.dat** tallennetaan seuraavat asetukset: **Resurssienhallinta** (Explorer), **Tehtäväpalkki** (Taskbar), **Kirjoittimen** asetukset, **Ohjauspaneeli** (Control Panel), **Apuohjelmien** asetuksia ja **Opas-**

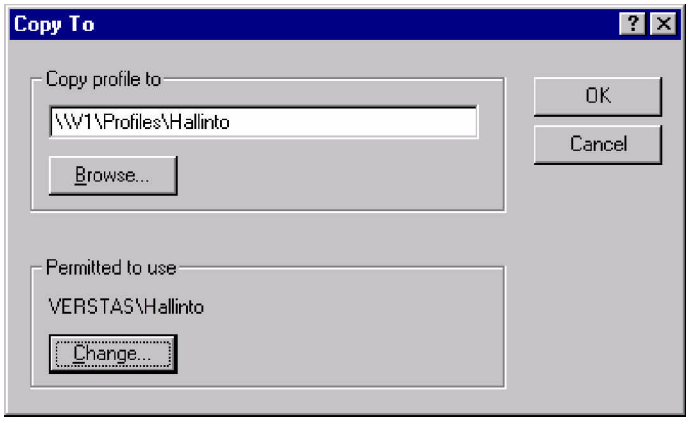
teen kirjanmerkit. Profiiliitiedoston tiedostonimi voi olla henkilökohtaisen profiilin (**NTUser.dat**) tai pakollisen käyttäjäprofiilin (**NTUser.man**) nimi.

Jos sekä Windows NT -työaseman **paikallinen käyttäjätunnus** että Windows NT -toimialueella määritelty käyttäjätunnus on sama, niin työaseman hakemistorakenteeseen tulee kaksi käyttäjätunnuksen mukaista hakemistoa, esimerkiksi **JKI** ja **JKI.000**.

Jos haluat määritellä käyttäjälle **palvelimella sijaitsevan** (*Roaming*) profiilin, määritä käyttäjäprofiilin sijainti **User Manager for Domainsissa** kirjoittamalla sen polku profiilin asetuksissa **User Profile Path** -ruutuun; polun on oltava **verkkopolku** annettuna UNC-nimellä, esimerkiksi **\\V1\PROFILES\JKI**.

Lisäksi mahdollisen työasemassa jo sijaitseva **paikallisen** (*Local*) profiilin tyyppi ja sijainti on muutettava työasemassa **Ohjauspaneelin** (Control Panel) **Järjestelmä** (System)-kuvakkeen avulla.

Käyttäjäprofiilit (User Profiles)-välilehden **Muuta tyyppi** (Change Type)- ja **Kopioi mihin** (Copy To)-painikkeilla voit muuttaa profiilin tyyppiä ja sijaintia. Anna myös käyttöoikeudet halutulle käyttäjälle tai käyttäjäryhmälle **Muuta** (Change)-painikkeella.



Jos haluat käyttöön **pakollisen profiilin**, jota käyttäjät eivät voi muuttaa, käy tämän jälkeen Resurssienhallinnalla muuttamassa kyseisessä hakemistossa **NTUser.dat** tunnisteelle **NTUser.man**. Tiedostotyyppi muuttuu samalla **MAN-tyyppiseksi**. Tiedostotyypin muutto aiheuttaa sen, että käyttäjä ei voi muuttaa profiiliaan. Tällöin viimeksi profiilia käyttänyt käyttäjä ei muuta (vahingossakaan) profiilin asetuksia.

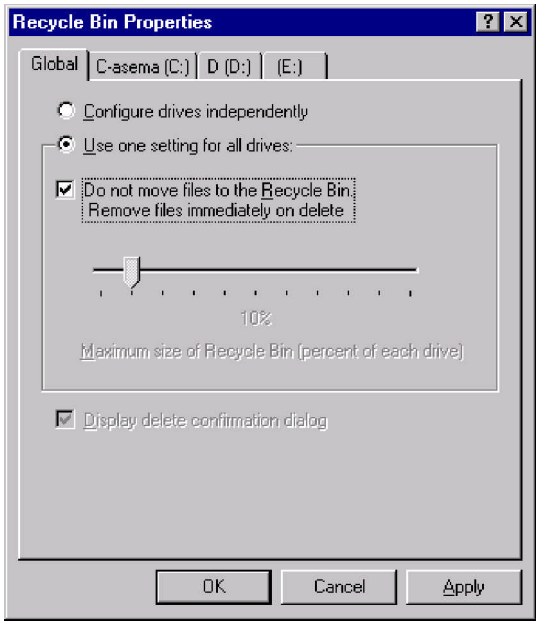
Anna lisäksi kyseiseen hakemistoon kyseiselle käyttäjäryhmälle tai käyttäjälle vain lukuoikeudet **Read**.

Jos suojaukset eivät ole kunnossa, niin palvelimella sijaitsevaan käyttäjän profiilihakemistoon saattaa päästä kiinni asiattomia käyttäjiä. Vaara piilee siinä, että jos käyttäjä tallentaa työpöydälleen dokumentteja, niin ne tallennetaan **Desktop** (Työpöytä)-hakemistoon. Jos hakemiston suojaukset eivät ole kunnossa, toinen käyttäjä voi päästä lukemaan näitä työpöydälle tallennettuja tiedostoja!

Roskakori (Recycle Bin)

Roskakori (Recycle Bin) tarjoaa palautusmahdollisuuden poistetuille tiedostoille. Siihen liittyy eräs tietosuojaongelma - on hyvä muistaa, että se on **käyttäjäkohtainen vain NTFS-levyillä**! FAT-levyillä **Roskakori** (Recycle Bin) on kaikille käyttäjille yhteinen!

Tallennus Roskakoriin voidaan ohittaa painamalla vaihtonäppäintä objektin poistamisen yhteydessä. Lisäksi se voidaan kytkeä pois käytöstä.



Asetukset voidaan antaa kaikille levyasemille tai per levyasema. **Roskakori** (Recycle Bin) ei tue levykkeitä tai verkkoasemia.

Kirjoittimien suojaaminen

Myös kirjoittimia voi suojata määrittämällä niille käyttöoikeuksia; ne määrittävät, millä tavalla yksittäinen käyttäjä tai käyttäjäryhmä voi käsitellä kirjoitinta. Jos kuulut käyttäjäryhmään, jolla on esimerkiksi tulostusoikeudet **Print** kirjoittimeen, voit tulostaa töitä kirjoittimella, mutta et voi kuitenkaan muuttaa kirjoittimen asetuksia.

Käyttöoikeudet määritellään valitsemalla kirjoittimen pikakuvakkeen **Sharing** tai valitsemalla **Properties** ja **Sharing** -välilehti.

Käyttöoikeudet

Security-välilehden **Permissions**-painikkeella voidaan antaa käyttäjille oikeuksia kyseiselle kirjoittimelle. Oikeudet **Type of Access**-listassa ovat seuraavat:

- **No Access** - ei käyttöoikeutta, jolloin kirjoittimelle ei voi tulostaa eikä kirjoitinta ei voi hallita
- **Print** - tulostaminen ja omistettujen tulostustöiden hallinnointi on mahdollista
- **Manage Documents** - kaikki **Print**-oikeudet sekä tulostusjonossa olevien töiden hallinta
- **Full Control** - kaikki **Manage Documents**-oikeudet sekä kirjoittimien jakaminen, ominaisuuksien muuttaminen, kirjoittimen poistaminen ja kirjoittimen käyttöoikeuksien muuttaminen.

Huomaa seuraavat seikat:

- Oletuksena **Everyone**-ryhmällä on tulostusoikeudet (**Print**), tulostustyön luoja tai omistaja **Creator-Owner** voi hallita täysin omaa tulostustyötään.
- Käyttöoikeudet täydentävät toisiaan; poikkeus on **No Access**, joka kumoaa kaikki muut käyttöoikeudet.

- Jos sinulla on tulostusoikeus (**Print**), sinulla on myös oikeus ohjata **omien töidesi** tulostamista. Kun luot tulostustyön, sinulla on siihen **Creator Owner** -käyttöoikeudet. Tavallisesti ei ole syytä muuttaa tätä käyttöoikeutta tai poistaa sitä käyttöoikeusluettelosta.

- Jotta voisit muuttaa kirjoittimen käyttöoikeuksia, sinun on oltava kirjoittimen omistaja tai sinulla on oltava käyttöoikeustaso **Full Control**.

- Jos yrität antaa **Everyone**-ryhmälle **No Access**-oikeudet, niin saat siitä ensin varoituksen! Tällaisen tarpeen voi kiertää suunnittelemalla käyttäjien ryhmät ja niiden oikeudet uudelleen.

Valvominen

Kirjoittimia valvomalla voit seurata niiden käyttöä. Voit valita valvottavan kirjoittimen, valvottavat ryhmät tai käyttäjät ja valvottavat toiminnot sekä onnistuneita että epäonnistuneita toimintoja. Kirjoittimen valvominen asetetaan valvottavan kirjoittimen kirjoitinikkunassa tai kuvakkeessa **Properties**- tai **File** | **Properties**-valinnalla **Security**-välilehden **Audit**-painike.

Tee halutut valvontamääritykset luettelon jokaiselle ryhmälle tai käyttäjälle valitsemalla ensin ryhmän tai käyttäjän nimi ja sitten valvottavat tapahtumat. Valitse lopuksi **OK**.

Kirjoittimen valvominen poistetaan valitsemalla ryhmän tai käyttäjän nimi ja sitten **Remove**-painike.

Omistus

Kirjoittimen luojasta (käyttäjä, joka sen on asentanut) tulee sen **omistaja**. Kirjoittimen omistaja voi aina muuttaa kirjoittimen käyttöoikeuksia. Jos sinulla on kirjoittimen käyttöoikeustaso **Full Control**, voit siirtää kirjoittimen omistuksen itsellesi; muussa tapauksessa sinun on kirjauduttava käyttäjätunnuksella, joka kuuluu **Administrators**-ryhmään.

Kirjoittimen omistuksen muuttaminen tehdään kirjoittimen kirjoitinikkunassa tai kuvakkeessa **Properties**- tai **File** | **Properties**-valinnalla **Security**-välilehden **Ownership**-painikkeella. Valitse **Take Ownership**-painike ja paina **Close**.

System Policy Editor

Järjestelmäkäytäntö (*System Policy*) tarkoittaa rekisterin määrityksiä, joilla voidaan rajoittaa entisestään Windows NT:n käyttöoikeuksia, asetusten muuttamista, verkkoon kirjautumista, salasanoja jne. Periaatteessa se toimii kuten Windows 95:n järjestelmäkäytäntökin, mutta ei ole yhteensopiva.

Asetukset menevät rekisteriin **HKEY_CURRENT_USER**- ja **HKEY_LOCAL_MACHINE** -avaimiin.

Järjestelmäkäytäntöjen käytännön toteuttamista on käsitelty **Luvussa 5**.

Järjestelmäkäytäntöjen etuja ovat:

- Asetusten suojaaminen - järjestelmäkäytäntöjä voidaan käyttää missä tahansa Windows NT 4.0 -mikrossa, myös ilman lähiverkkoa
- Lähiverkkoa käytettäessä voidaan keskittää asetukset ja hallita asetuksia keskitetysti **NTConfig.POL-tiedoston** avulla
- Rekisterin asetusten muuttaminen on selkeämpää kuin käytettäessä rekisterieditoria
- Asetukset voidaan ottaa käyttöön paikallisella tasolla, jolloin jokaisella mikroa käyttävällä on samat asetukset
- Asetuksissa voidaan määritellä oikeudet Ohjauspaneeliin ja sen objektien asetusten muuttamiseen, työpöytään ja sen objekteihin sekä näiden objektien muokkaamiseen ja verkon asetuksiin
- Asetuksissa voidaan tukeutua lähiverkkoon, jolloin **käyttäjäprofiilien** ja käyttäjätunnusten avulla **käyttäjäkohtaiset** asetukset seuraavat käyttäjää, kirjoitautuipa hän verkkoon miltä työasemalta tahansa
- Voidaan ottaa käyttöön lisäksi käyttäjäryhmäkohtaiset ja työasemakohtaiset asetukset.

Helpotat järjestelmäkäytäntöjen käyttöä seuraavasti:

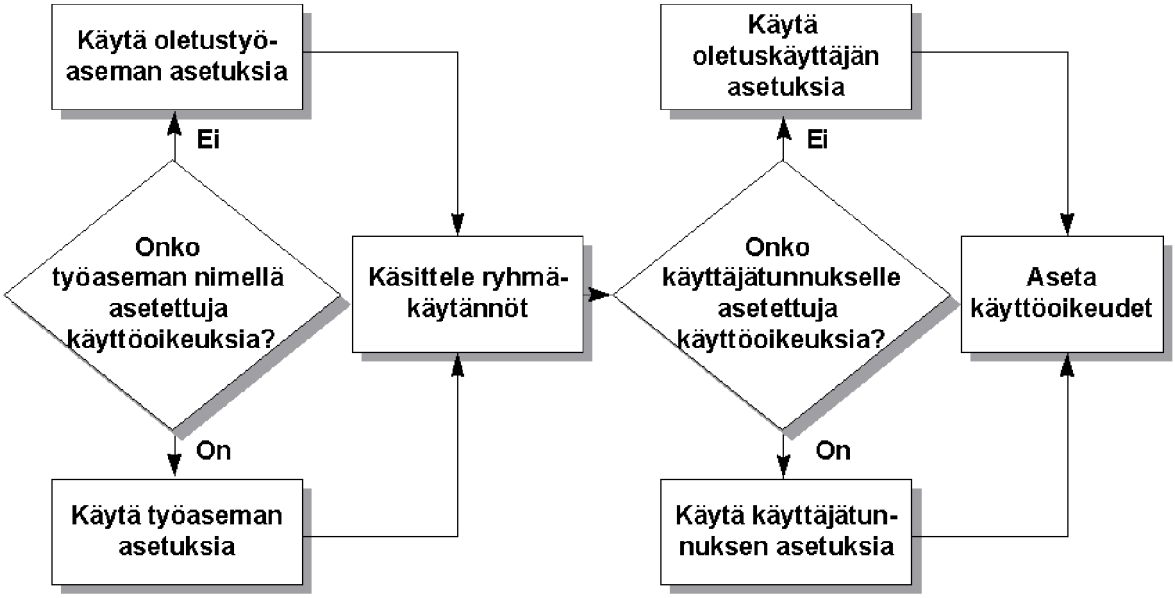
- Järjestelmäkäytäntöjen käyttöönotto on harkittua ja testattua
- Tunnet itsekin järjestelmäkäytäntöjen idean ja toteutuksen
- Testaillessasi toimintoa ota varmistukset rekisteristä
- Ole varovainen! Testaa kaikki asetukset huolellisesti eri käyttäjätunnuksilla ja eri työasemissa!
- Määrittele etäpäivitys käyttöön paikallisiin järjestelmäkäytäntöihin. Jos käyttäjiä / työasemia on useita kymmeniä, palvelimen / verkon tulisi olla tehokas. Seuraa verkon ja palvelimien kuormitusta!
- Seuraa Windows NT -palvelimella lokien avulla **NTCONFIG.POL**-tiedostojen käyttöä!

Järjestelmäkäytäntöjen periaate on syytä ymmärtää hyvin, jotta ne voi ottaa käyttöön eikä sattuisi kömmähdyksiä. Seuraavat seikat vaikuttavat järjestelmäkäytäntöihin:

- **Oletuskäyttäjän** (Local User) ja **Oletustietokoneen** (Local Computer) asetukset. Nämä ovat itse asiassa paikallisen rekisterin asetuksia
- Onko **työasemalle** luotu profiili. Tässäkin on varminta käyttää Windows NT:n verkkotukea ja sen oletuksia (**NTConfig.POL**)
- Kuuluuko käyttäjä johonkin **käyttäjäryhmään**, jolle on määritelty järjestelmäkäytäntöjä. Näiden voimaantulolla on oma järjestyksensä!

NTConfig.POL-tiedosto on System Policy Editorilla luotavissa oleva tiedosto, jonka Windows NT 4.0 osaa lukea verkon palvelimelta automaattisesti. Muuten voidaan luoda käyttäjäkohtainen POL-tiedosto, joka otetaan käyttöön UNC-polun takaa ns. **manuaalisella päivityksellä**, esimerkiksi **\\V1\Policy\JKI.POL**.

Oletuksena Windows NT 4.0 pyrkii lataamaan **NTConfig.POL**-tiedoston Windows NT -palvelimen **NETLOGON** -hakemistosta. Käyttäjällä tai käyttäjäryhmällä ja työasemalla voi olla omat asetuksensa. Ne voidaan tallentaa suoraan **NTConfig.POL**-tiedostoon. Tällöin käsittelyjärjestys on seuraava:



Voit käyttää **System Policy Editoria** kahdessa eri tilassa:

- Työaseman **paikallisen rekisterin** tai **etähallitun työaseman rekisterin** käsittelyssä. Tällöin asetukset menevät samantien kyseisen työaseman rekisteriin! Tällöin käsitellään paikallisen rekisterin asetuksia. Kyseinen työasema on käynnistettävä uudelleen, jotta asetukset tulevat voimaan

- **Järjestelmäkäytäntötiedostojen** (.**POL**) muokkaamiseen. Näitä voit luoda aivan vapaasti, mutta suosittelen noudattamaan Windows NT:n oletuksia! Tämä on ns. *Policy File Mode*

Käyttäjälle muokattavissa olevia asetuksia ovat seuraavat:

- Näytön **Display** asetusten muuttamisen

- Työpöydän **Desktop** taustakuva ja värimallin asetukset

- Liittymän **Shell** asetukset:
  - Työpöydän **Custom Folders** mahdollistaa käyttöliittymän asetusten muuttamisen tavallisesti viittaamalla muuhun kuin oletushakemistoon
  - Rajoitukset **Restrictions**, joilla voidaan poistaa käytöstä mm. **Käynnistä** (Start)-valikon valintoja
- **System** - rekisterin asetusten muuttaminen.

Työasemalle muokattavissa olevia asetuksia ovat seuraavat:

- **Network** -verkkoasetukset - **Update** päivitysasetus on oleellinen, koska jos oletustietokoneen **Local Computer** asetuksissa on valittu etäpäivitys **Remote Update**, rekisteriä voidaan päivittää automaattisesti palvelimelta: tiedosto **NTCONFIG.POL** etsitään Windows NT -palvelimen **NETLOGON** -hakemistosta. Oletusta voi muuttaa valitsemalla päivitystilakohtaan **Update Mode** tyypiksi **Manual**. Voit myös valita **Display error messages**, jolloin virheilmoitukset tulevat näyttöön.
- **Kuormituksen tasaus** Load Balance toimii siten, että koska **pääohjauskoneen** (Primary Domain Controller) **NETLOGON**-hakemistoa monistetaan toimialueen **ohjauskoneiden** (*Backup Domain Controller*) kesken, voidaan **NTCONFIG.POL** ladata myös siltä ohjauskoneelta, joka hyväksyi käyttäjän verkkoonkirjautumisen.

Voit asentaa **System Policy Editorin** Windows NT 4.0 -palvelimen CD-ROM:ilta **Clients\Srvtools\Winnt**-kansiosta komennolla **SETUP**.

Työaseman **paikallisen rekisterin** tai **etähallitun työaseman rekisterin** käsittelyssä toimitaan seuraavasti:

1) Valitse **File** | **Open Registry**. Jos haluat avata toisen työaseman rekisterin, valitse **Connect** ja anna toisen työaseman nimi

2) Näyttöön tulee paikallinen rekisteri oletuskäyttäjineen.

3) Tee halutut asetukset ja tallenna tiedosto. Asetukset tulevat voimaan työaseman käyttäjille käynnistyksen jälkeen.

C2 Configuration Manager

National Security Agencyn (NSA) C2-luokitus viittaa turvaohjeisiin, joissa määritetään turvallisen järjestelmän toimintaa. Windows NT on NSA:n EPL-listalla (*Evaluated Programs List*, arvioitujen tuotteiden luettelo). EPL-listalla oleminen tarkoittaa, että Windows NT -käyttöjärjestelmän avulla **voidaan** saavuttaa C2-turvallisuusluokitus omassa järjestelmässä.

C2-sertifiointi pätee nimittäin vain täydelliseen kokoonpanoon, joka sisältää käyttöjärjestelmän lisäksi laitteiston, ohjelmat ja ympäristön, johon järjestelmä asennetaan.

Windows NT 4.0 Resource Kitin **C2 Configuration Manager** (C2CONFIG.EXE) on apuohjelma, jolla voidaan vertailla nykyisiä asetuksia C2-tason vaatimuksiin ja tarvittaessa suorittaa tarvittava konfigurointi.- **C2 Configuration Managerin** mukana tulee .H-tiedosto, joten voit tarvittaessa kirjoittaa omia laajennuksia sovellukseen DLL:ien avulla.

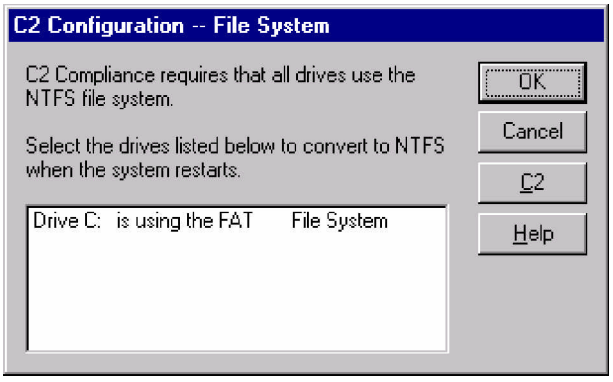
Tarkistettavat asetukset ovat:

- File Systems
- OS Configuration
- OS/2 Subsystem
- Posix Subsystem
- Security Log
- Halt on Audit Failure
- Display Logon Message
- Last Username Display
- Shutdown Button
- Password Length
- Guest Account
- Networking
- Drive Letters & Printers
- Removable Media Drives
- Registry Security
- File System Security
- Other Security Items

Nämä ominaisuudet saadaan käyttöön myös sopivalla valvontatyökalulla tai suoraan rekisterin asetuksilla, joten niiden esitteleminen tarjoaa hyvän katsauksen NT:n keskeisiin suojausasetuksiin.

File Systems

Tämän asetuksen avulla voit tarkistaa kiintolevyjen tiedostojärjestelmät. Vain NTFS takaa riittävän tietosuojan. Muiden tiedostojärjestelmien (NTFS:n lisäksi voi olla vain FAT Windows NT 4.0:ssa) aiheuttamat aukot suojauksissa ilmoitetaan luettelossa.

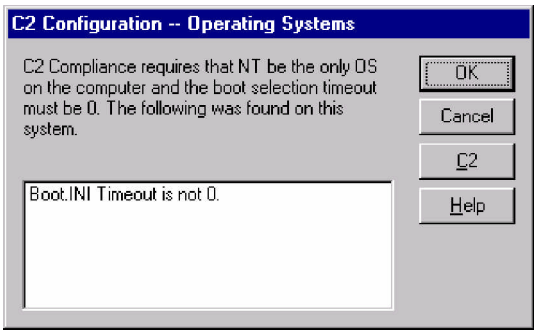


Voit **CONVERT**-komennolla muuntaa FAT:n NTFS-tiedostojärjestelmäksi.

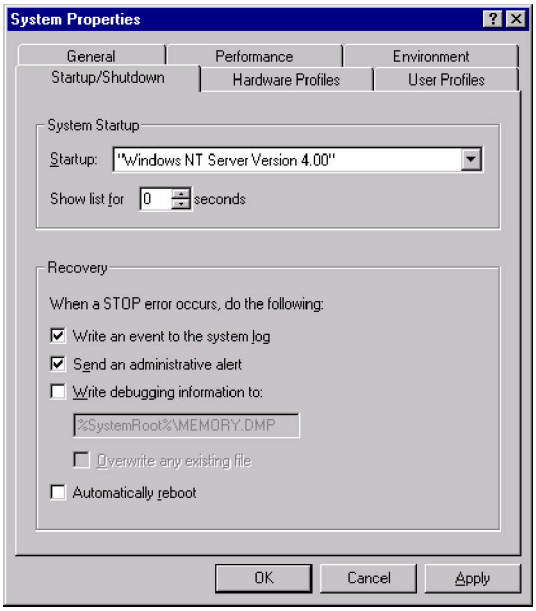
Muista, että sopivalla käynnistyslevykkeellä voidaan korkata NTFS. Samoin siirtämällä kiintolevy toiseen NT-koneeseen tai asentamalla NT uudelleen. Suojaa siksi NT-kone myös fyysisesti.

OS Configuration

Jos oletuskäyttöjärjestelmä **ei** ole NT ja jos odotusaika ei ole **0 sekuntia**, siitä saadaan ilmoitus.

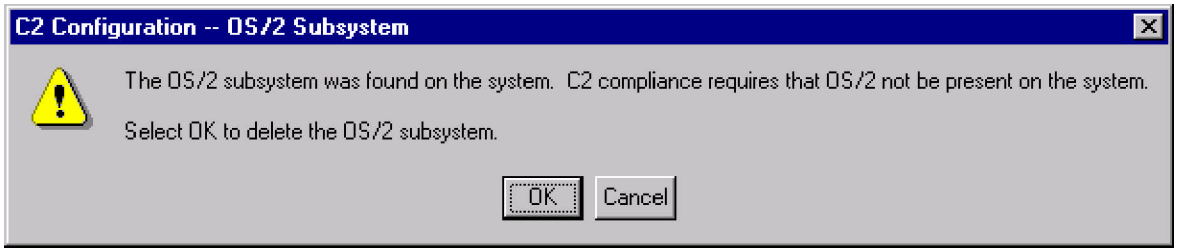


Asetus annetaan **Boot.INI**-tiedostossa, mutta sitä voi käsitellä suoraan Ohjauspaneelin **System**-kuvakkeella.



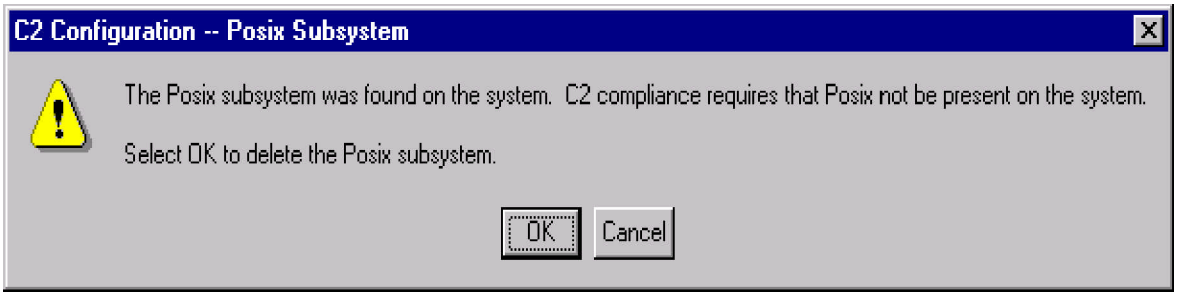
OS/2 Subsystem

C2-taso edellyttää, että OS/2-alijärjestelmää **ei** löydy NT-koneesta. Sen voi poistaa painamalla **OK**.



Posix Subsystem

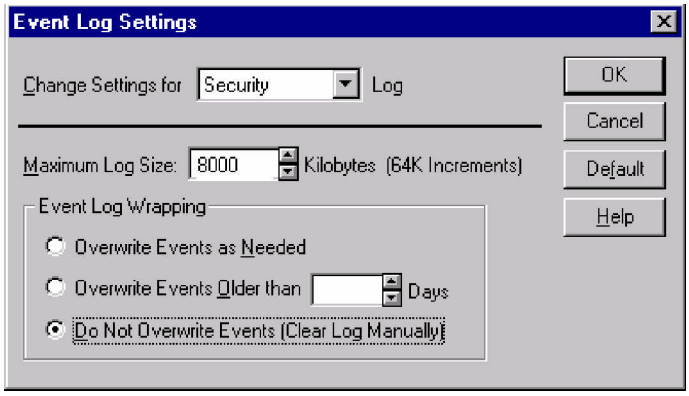
C2-taso edellyttää, että POSIX-alijärjestelmää **ei** löydy NT-koneesta. Sen voi poistaa painamalla **OK**.



Security Log

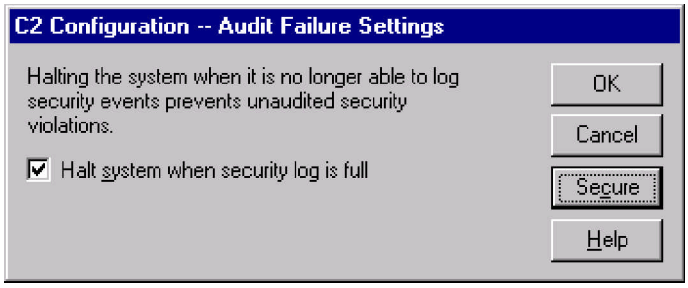
C2-taso edellyttää, että suojauslokia ei tyhjennetä (tai kirjoiteta tapahtumien päälle) automaattisesti. Painamalla **C2** asetetaan päälle lokin tyhjentäminen vain erikseen niin haluttaessa.

Saman voit tehdä Event Viewerin lokin suojauslokin asetuksilla. Muista asettaa lokille riittävän iso koko!



Halt on Audit Failure

Tällä asetuksella varmistetaan taatusti, että tapahtumat myös menevät lokiin - lokin täyttyessä nimittäin NT jysähtää! Asetuksen saa päälle valitsemalla **Halt system when security log is full** tai painamalla **Secure**.



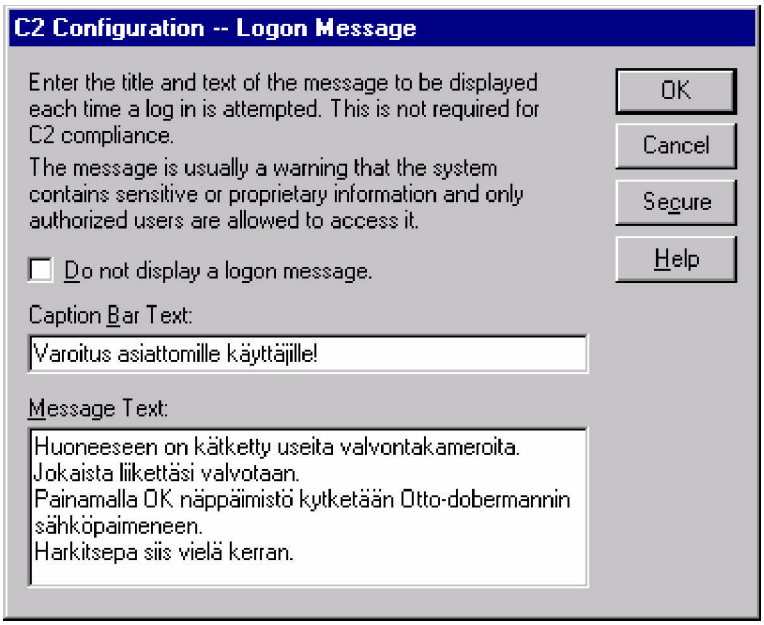
Saman voit tehdä asettamalla rekisteriin **CrashOnAuditFail**:in:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Lsa**
Nimi	**CrashOnAuditFail**
Tyyppi	**REG_DWORD**
Arvo	**1** - jysähtää kun loki on täynnä, **2** Administrator voi kirjautua (arvo kertoo myös, että jysähdyksen syy oli lokin täyttyminen). Arvoa **0** ei ole

Poista tarvittaessa nimi. Muista myös päivittää **Emergency Repair Disk** (ERD).

Display Logon Message

Asetuksella saadaan käyttöön ilmoitus, joka käyttäjän on hyväksyttävä, ennen kuin kirjautuu järjestelmään. Tämä ei ole kuitenkaan C2-luokituksen vaatimuksissa.



Asetus on rekisterissä, jonne sen voit suoraan asettaa tarvittaessa.

Otsikkoteksti:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**LegalNoticeCaption**
Tyyppi	**REG_SZ**
Arvo	Oletus on tyhjä. Voit kirjoittaa merkkijonon, joka tulee näkyviin ikkunan otsikkona kirjauduttaessa järjestelmään

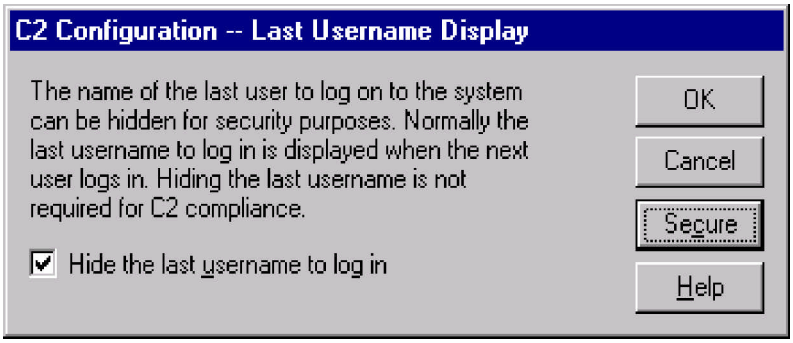
Ilmoitus:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**LegalNoticeText**
Tyyppi	**REG_SZ**
Arvo	Oletus on tyhjä. Voit kirjoittaa merkkijonon, joka tulee näkyviin ikkunassa kirjauduttaessa järjestelmään

Last Username Display

Edellisessä kirjautumisessa käytetty tunnus voidaan myös piilottaa. Se ei ole C2-vaatimuksissa.

Asetuksen saa päälle valitsemalla **Hide the last username to log in** tai painamalla **Secure**.

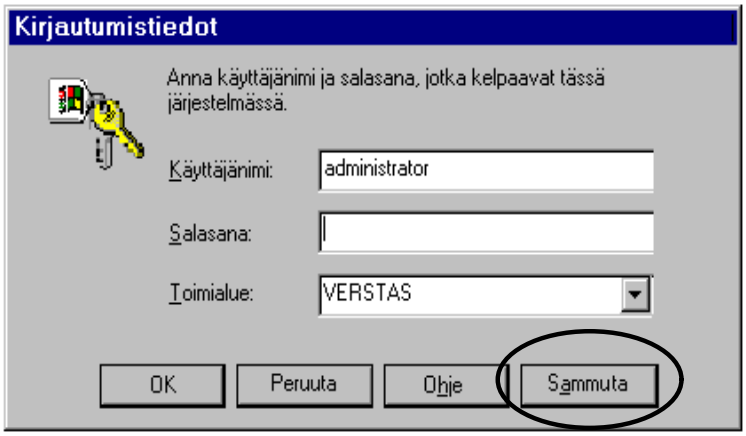


Asetus tallennetaan rekisteriin, ja ilman **C2 Configuration Manageria** edellisen kirjautumisen asetukset määritellään suoraan rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**DontDisplayLastUserName**
Tyyppi	**REG_SZ**
Arvo	Oletus on **0**. Jos muutat arvon **1**:een (*true*), **Käyttäjätunnus** (Username) jää tyhjäksi. Nimi on lisättävä tarvittaessa

Shutdown Button

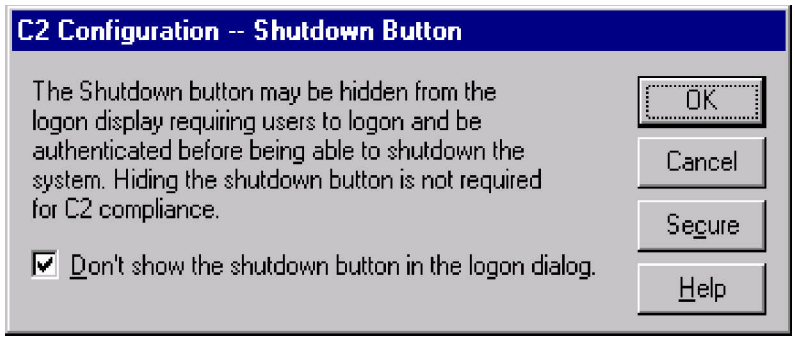
Shutdown-nappulan voi myös piilottaa, jolloin käyttäjän on kirjauduttava voidakseen ajaa järjestelmän alas. Tämä ei ole C2-vaatimuksissa.



Asetukset määritellään suoraan rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**ShutdownWithoutLogon**
Tyyppi	**REG_SZ**
Arvo	**0 tai 1**; oletus **0** Serverissä, oletus **1** työasemassa. Muuttamalla palvelimessakin asetus **1**:ksi voidaan lisätä myös palvelimeen **Welcome**-ikkunaan **Shutdown**-valinta. Tällöin palvelin voidaan-kin ajaa alas ilman sisäänkirjautumista

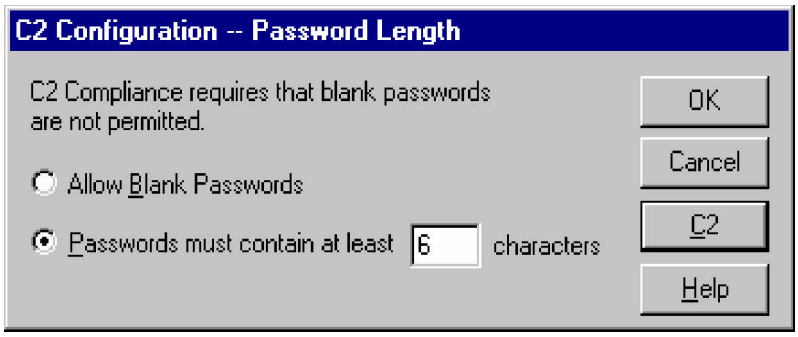
Asetuksen saa päälle **C2 Configuration Managerilla** valitsemalla **Don t show the shutdown button in the logon dialog** tai painamalla **Secure**.



Password Length

Salasanan minimipituus C2-luokituksessa on 6 merkkiä. Asetus annetaan tyypillisesti **User Manager for Domains:ssa**.

Asetuksen saa päälle valitsemalla **Passwords must contain at elast 6 characters** tai painamalla **C2**.

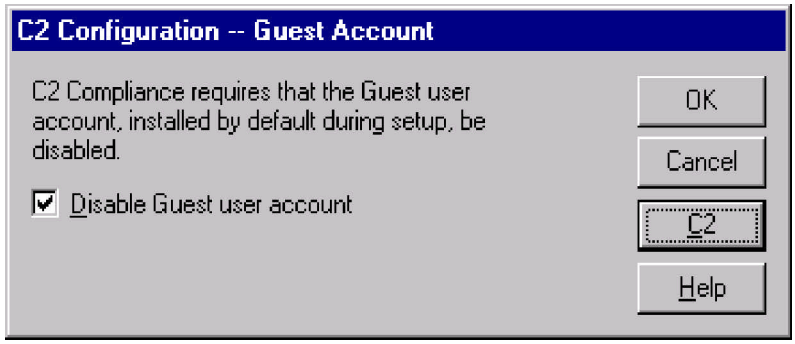


Guest Account

Guest (Vieras)-tunnukseen sisältyy eräs suurimmista NT:n suojausriskeistä. Oletuksena tunnus on voimassa NT-työasemissa, mutta ei NT-palvelimissa tai NT-toimialueilla. Guest-tunnuksen poistaminen ei kuitenkaan vielä takaa täydellistä tietosuojaa! On siis äärimmäisen vaarallista tuudittautua luuloon, että pelkästään tunnuksen poistaminen käytöstä (disablointi) lisäisi oleellisesti järjestelmän suojauksia. Vaatimus tunnuksen poistamisesta käytöstä on C2-luokituksen mukainen.

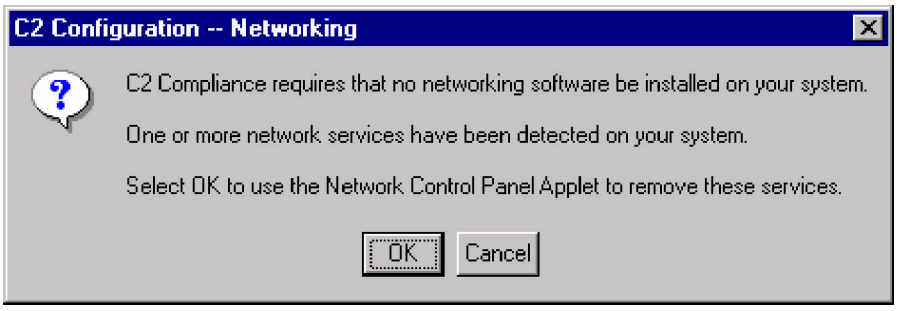
Tunnuksen poistaminen käytöstä annetaan tyypillisesti **User Manager for Domains:ssa**.

Asetuksen saa päälle valitsemalla **Disable Guest user account** tai painamalla **C2**.



Networking

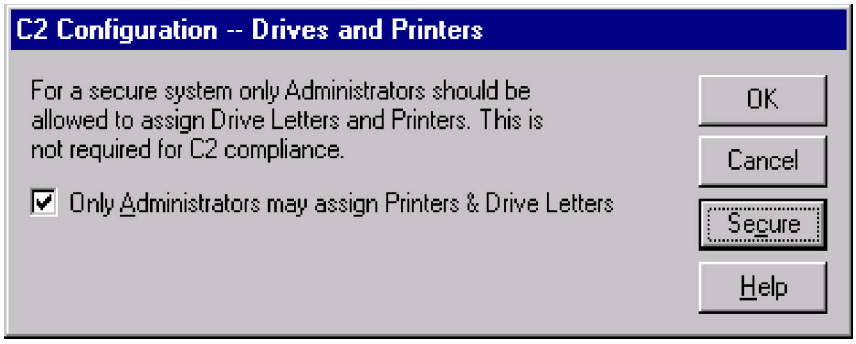
Vaatimus verkkokomponenttien poistamisesta käytöstä on C2-luokituksen mukainen, mutta tietysti hieman ontuu NT-palvelmien kohdalla. NT-työasemissa verkkokomponentit voi poistaa **Ohjauspaneelin** (Control Panel) **Verkko** (Network)-kuvakkeella.



Drive Letters & Printers

Lisäsuojauksena vain pääkäyttäjät voivat asettaa levyasematunnuksia ja kirjoittimia. Tämä ei ole C2-vaatimuksissa.

Asetuksen saa päälle valitsemalla **Only Administrators may assign Printers & Drive Letters** tai painamalla **Secure**.



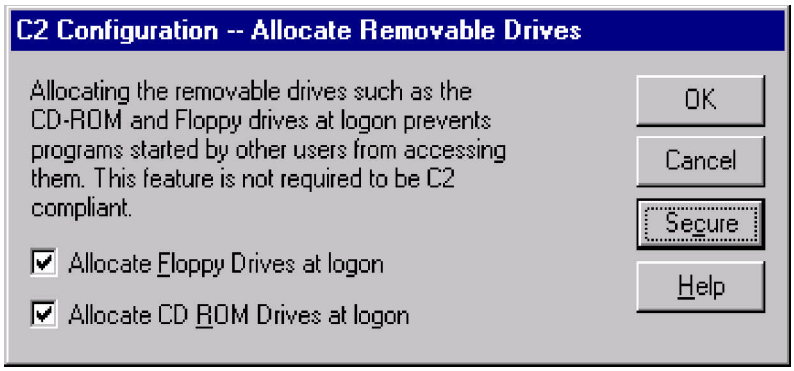
Removable Media Drives

Kaikilla käyttäjillä on oletuksena oikeudet käyttää levyke- ja CD-ROM-asemia. Jos halutaan estää tilanne, jossa verkon kautta käyttäjä on ottanut esimerkiksi levykeaseman käyttöönsä (jolla voi olla vain FAT-tiedostojärjestelmä) ja paikallisesti kirjautunut käyttäjä vaihtaa levyk-

keen (jolloin verkon kautta päästään käsiksi levykkeen tiedostoihin), voidaan antaa oikeudet vain paikallisesti kirjautuneelle käyttäjälle.

Tämä ei ole C2-vaatimuksissa.

Asetuksen saa päälle valitsemalla **Allocate Floppy Drives at logon** ja/tai **Allocate CD-ROM Drives at logon** tai painamalla **Secure**.



Asetukset määritellään suoraan rekisterissä. Levykeasemat:

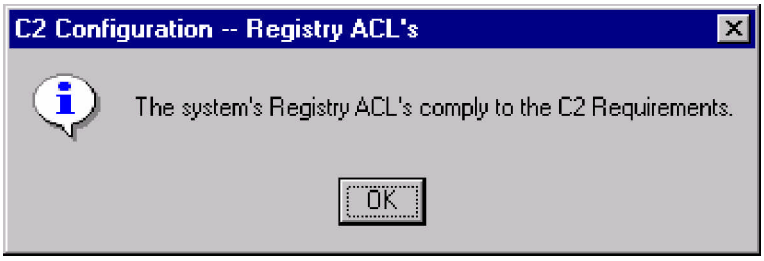
Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**AllocateFloppies**
Tyyppi	**REG_SZ**
Arvo	**0 tai 1**; oletus **0,** muuttamalla asetus **1**:ksi annetaan käyttöoikeus vain paikallisesti kirjautuneelle käyttäjälle

CD-ROM-asemat:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**AllocateCDRoms**
Tyyppi	**REG_SZ**
Arvo	**0 tai 1**; oletus **0,** muuttamalla asetus **1**:ksi annetaan käyttöoikeus vain paikallisesti kirjautuneelle käyttäjälle

Registry Security

Voit asettaa rekisteritietokannan käyttöoikeusluettelot C2-vaatimusten mukaisiksi. Jos asetukset ovat jo kunnossa, saat ilmoituksen:



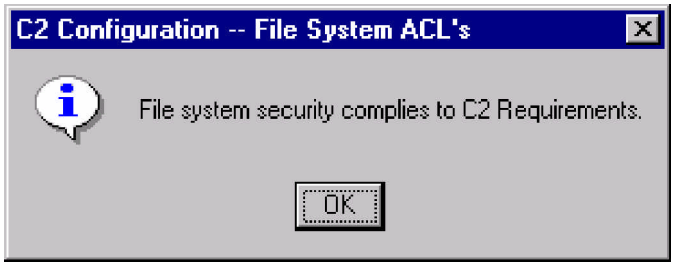
Muussa tapauksessa tarjotaan mahdollisuus asettaa rekisteritietokannan käyttöoikeusluettelot C2-vaatimusten mukaisiksi. Paina **OK**:

Tämän jälkeen varsinainen prosessi käynnistetään painamalla **OK**:

Rekisterin käyttöoikeusluettelot asetetaan tiedoston **C2REGACL.INF** mukaisiksi.

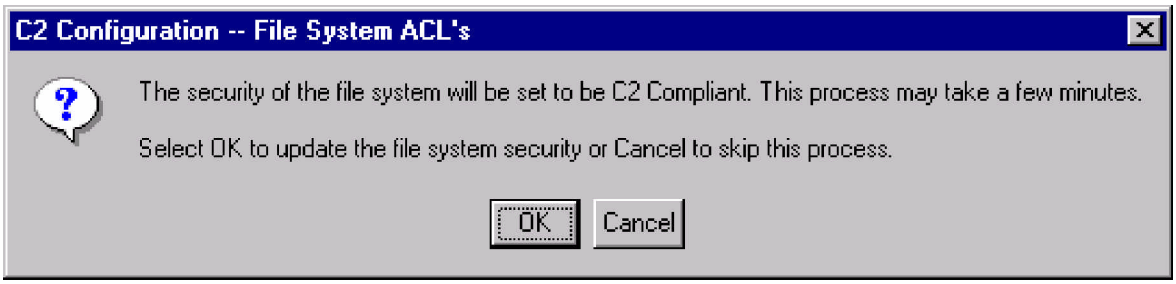
File System Security

Voit asettaa tiedostojärjestelmän asetukset järjestelmähakemistossa C2-vaatimusten mukaisiksi. Jos asetukset ovat jo kunnossa, saat ilmoituksen:



Muussa tapauksessa tarjotaan mahdollisuus asettaa tiedostojärjestelmät C2-vaatimusten mukaisiksi. Paina **OK**:

Tämän jälkeen varsinainen prosessi käynnistetään painamalla **OK**:

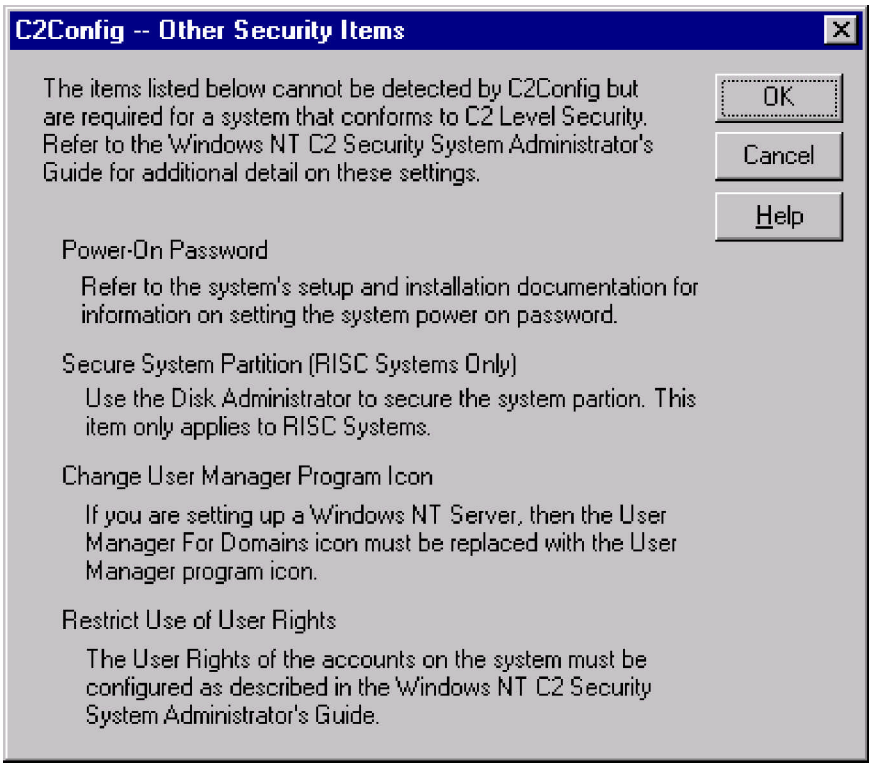


Järjestelmähakemiston käyttöoikeusluettelot asetetaan tiedoston **C2NTFACL.INF** mukaisiksi.

Other Security Items

Lopuksi saat listan asetuksista, jotka on syytä tarkistaa erikseen, sillä **C2 Configuration Manager** ei niitä pysty tarkistamaan saati asettamaan:

- **Power-On Password** - tietokoneen CMOS Setupissa asetettava BIOS-salasana
- **Secure System Partition** - RISC-tietokoneissa järjestelmälevyn suojaaminen
- **Change User Manager Program Icon** - muuta **User Manager for Domains** (USRMGR.EXE) -kuvake **User Managerin** (MUSRMGR.EXE) kuvakkeeksi
- **Restrict Use of User Rights** - rajoita käyttöoikeuksia. Katso lisäohjeita **Windows NT C2 Security System Administrator s Guide**-kirjasta.



Suojaustyökaluja

Windows NT -ympäristön reaaliaikaiseen valvontaan tulee jo NT:n mukana joitakin työkaluja:

- **Remote Access Admin**, jonka avulla voit hallita myös NT-palvelimen tai minkä tahansa NT-työaseman etäkäyttöpalvelua**.** Käyttökelpoisuus tietoturvan kannalta perustuu reaaliaikaiseen etäkäytön seuraamiseen ja tarvittaessa käyttäjän yhteyden katkaisemiseen tai palvelun ajamiseen alas verkon kautta

- **Performance Monitor**, jonka avulla voit seurata myös NT-palvelimen tai minkä tahansa NT-työaseman suorituskykyä työasemasta. Tämän käyttökelpoisuus tietoturvan kannalta perustuu reaaliaikaiseen resurssien kuormituksen seuraamiseen ja hälytysten lähettämiseen tai komentojen käynnistämiseen. Sopivasti viritettynä kohtuullinen työkalu, koska toimintaa voidaan räätälöidä ja automatisoida

- **Event Viewer**, jonka avulla voit seurata NT-palvelimen tai minkä tahansa NT-työaseman tapahtumalokia. Varsinkin suojauslokin tallennus ja siirtäminen tehokkaampien työkalujen analysoitavaksi suositeltavaa. Voidaan jossain määrin automatisoida

- **Windows NT Diagnostics**, jonka avulla voit seurata myös NT-palvelimen tai minkä tahansa NT-työaseman laitteistoasetuksia omasta työasemastasi. Käyttökelpoisuus tietoturvan kannalta perustuu reaaliaikaiseen laiteohjainten ja palveluiden seuraamiseen, mutta edellyttää manuaalisia operaatioita

- **Server Manager**, palvelimen hallinta, jonka käyttökelpoisuus tietoturvan kannalta perustuu reaaliaikaiseen resurssien seuraamiseen. Edellyttää manuaalisia operaatioita.

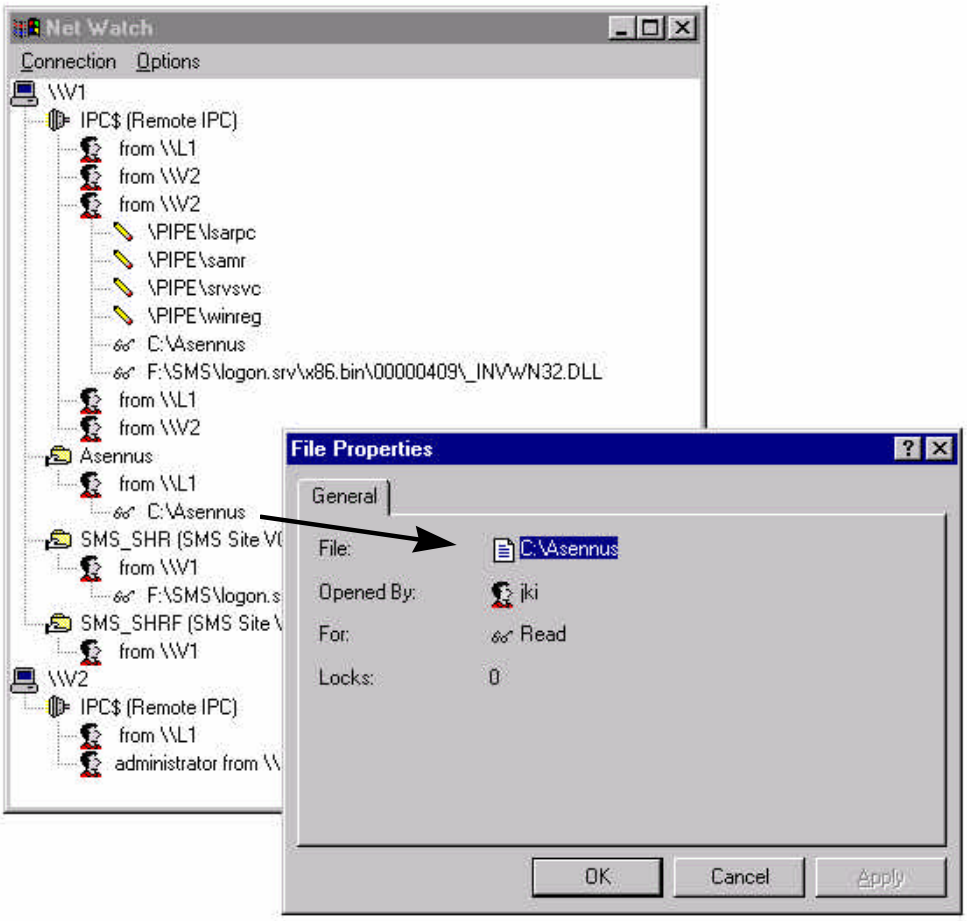
Tarpeellisia työkaluja ovat tyypillisesti näiden lisäksi seuraavanlaiset:

- Porttien tutkijat (Port scanners)
- Puhelinyhteyksien tutkijat (Dial-up scanners)
- Tapahtumalokien analysointiohjelmat (Event log analyzers)
- Rekisterien analysointiohjelmat (Registry analyzers)
- Käyttöoikeusluettelojen analysointiohjelmat (Access control analyzers)
- Protokolla-analysaattorit ja pakettien tutkijat (Protocol analyzers, packet sniffers)
- Yleiset suojausten tutkimisohjelmat (Overall security scanners).

Joitakin näistä tulee myös Resource Kitin mukana, esimerkiksi käyttöoikeuksien hallintaan **FIXACLS**, **PERMCOPY**, **PERMS**, **SCOPY**, **SUBINACL** ja **XCACLS**.

Net Watch

Net Watch on Resource Kitin apuohjelma, jolla voit tarkastella verkon NT-koneiden jaettujen resurssien käyttöä.



Net Watch ei korvaa **Server Manageria**, mutta toimii tarvittaessa mukavasti sen rinnalla.

Connection-valikosta voit antaa seuraavat valinnat:

- **Properties** - näet valitun kohteen ominaisuudet, esimerkiksi kauanko käyttäjä on käyttänyt a.o. resurssia
- **Add Computer** - lisää NT-koneen valvottavien listalle
- **Disconnect** - kytkee käyttäjän irti resurssista

- **Manage Shares** - jaettujen resurssien hallinta (saman saa tehtyä Server Managerilla)
- **Connect Network Drive** - kytkee levyasematunnuksen jaettuun resurssiin
- **Disconnect Network Drive** -katkaisee levyasematunnuksen yhteyden jaettuun resurssiin.

Options-valikosta voit valita:

- **Show Open Files** - näytetäänkö avoimet tiedostot
- **Show Hidden Shares** - näytetäänkö piilotetut jaetut resurssit
- **Show In Use Shares Only** - näytetäänkö vain käytössä olevat jaetut resurssit.

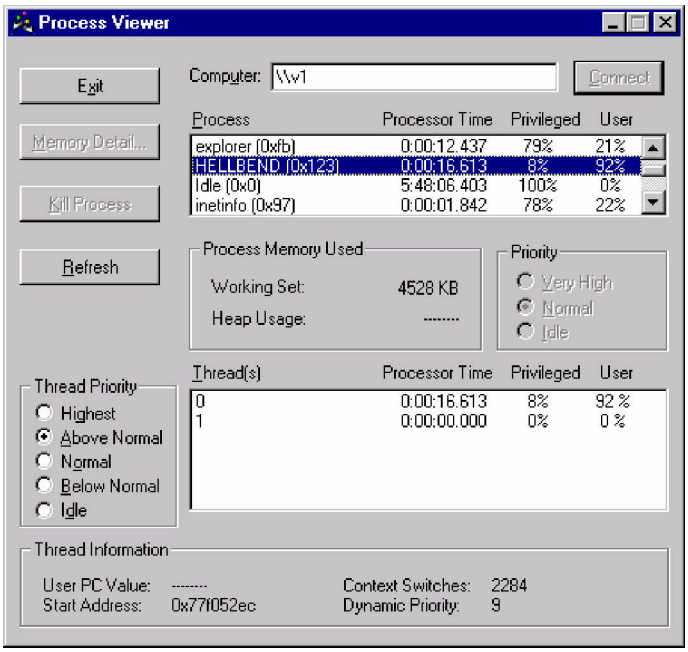
Process Viewer

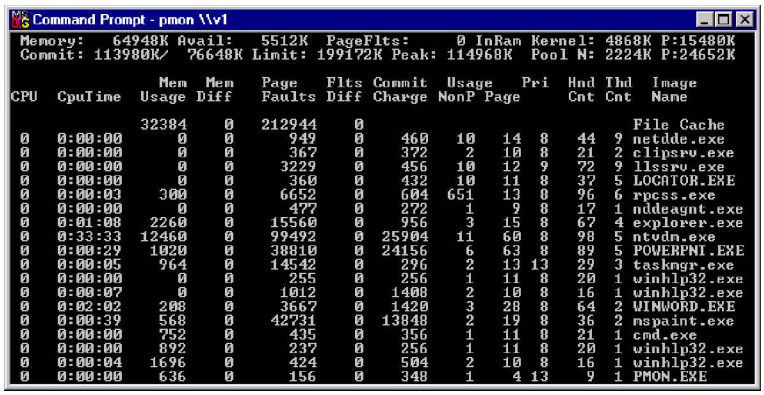
Resource Kitin **Process Viewerin** avulla voit valvoa (myös) toisessa NT-koneessa ajettavia prosesseja. Koneen nimen voi antaa **Computer**-kohtaan tai selata verkosta. 16-bittiset sovellukset ajetaan **ntvdm**:ssä (joista nähdään vain säikeen nimi), mutta esimerkiksi 32-bittinen **HellBender**-peli näkyy omalla nimellään!

Pmon

Resource Kitin **Pmon** on komentorivin ohjelma, jolla voidaan tutkia kohdekoneen prosesseja. Myös muistin käytöstä saadaan samalla yhteenveto. Komento on

pmon \\[kohde]

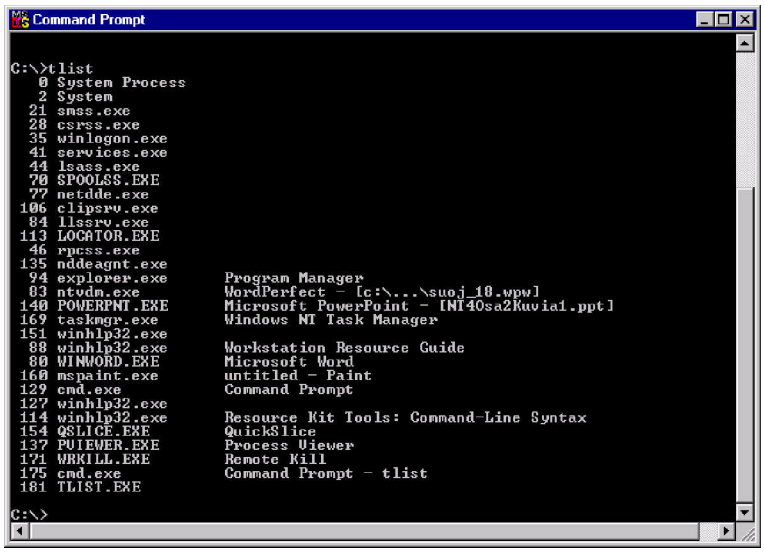




Tlist ja Kill

Tlist on Resource Kitin apuohjelma, jolla saadaan tehtäväluettelo (Task List) eli paikallisessa NT-koneessa ajettavien prosessien luettelo. Prosesseista nähdään prosessin **id-numero** (PID), jonka avulla voidaan lopettaa prosessi **Kill**-komennolla. Syntaksi on

Kill [PID]



Tässä esimerkissä komentojono suorittaa **Tlist-komennon** suodatetun tulostuksen ohjaamisen **FileName**-ympäristömuuttujassa määritettyyn hakemistoon, vain jos listassa on ympäristömuuttujassa **Pelit** määritettyjä **DOOM**-, **DUKE**- tai **HELLBEND**-merkkijonoja:

```
@echo off
SET FileName=\\V2\Lokit\%username%.%userdomain%.txt
SET TempFile=%Temp%\temp.txt
SET Pelit=DOOM DUKE HELLBEND
CD %Temp%
tlist > %TempFile%
findstr "%Pelit%" %TempFile% > nul
if errorlevel 1 goto loppu
findstr "DOOM" %TempFile% > %FileName%
echo %computername%  >> %FileName%
now >> %FileName%
:loppu
```

Tiedostonimi on asetettu ympäristömuuttujassa **FileName**, ja näillä asetuksilla se on esimerkiksi **JKI.VERSTAS.TXT**. Tiedostoon (jonka formaatti ei ole hirveän tyylikäs) tuodaan **prosessin id**:n numero ja nimi, **NT-koneen nimi** ja **päiväys**. Päiväys saadaan Resource Kitin **Now**-apuohjelmasta:

```
 348 ntvdm.exe        DOOM2.EXE - FROZEN
V1
```

Tue May 27 18:08:06 1997

Tätä voisi lähteä edelleen parantelemaan:

- **findstr "DOOM" %TempFile% > %FileName%** -rivin tilalle voisi laittaa **SHUTDOWN /L /R /T:10 Lopetetaanpas se pelien pelailu! /Y**-rivin, joka ajaa NT-koneen alas

- **Findstr**-ohjelmaan voisi syöttää etsittävät nimet **/G:[tiedostonimi]** -parametrilla, joka viittaa palvelimen hakemistoon

- Toisaalta ympäristömuuttujat voisi alustaa palvelimelta, esimerkiksi **CALL \\V2\Lokit\Pelit.BAT**

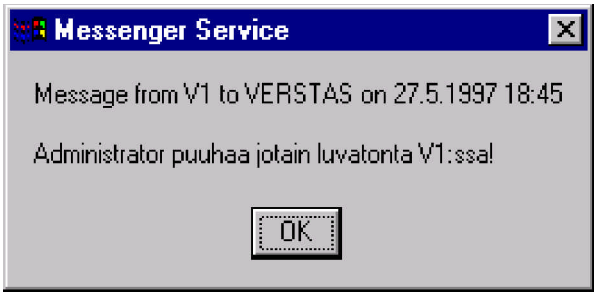
- Kolmas vaihtoehto olisi ajaa koko komentojono suoraan palvelimelta, mielellään UNC-nimellä (esimerkiksi **CALL \\V2\Lokit\GameChk.bat**)

- Komentojonon automaattiseen käynnistykseen voisi ajatella **Resource Kitin AutoExNT**-palvelua

- NT-koneessa voisi ajaa **Rkillsrv** -palvelua, jolloin tietämällä NT-koneen nimen voisi ajaa kyseisen prosessin alas. Tässä tarvitaan taas prosessin numeroa, mutta sehän jo tiedetäänkin!

Tyylikäs tapa on tietysti kertoa kaikille **NET SEND**-komennon avulla, mitä tietyllä NT-koneella puuhataan:

```
@echo off
SET TempFile=%Temp%\temp.txt
tlist > %TempFile%
findstr DOOM DUKE HELLBEND %TempFile% > nul
if errorlevel 1 goto loppu
net send * "%Username% puuhaa jotain luvatonta %Computername%:ssa!"
:loppu
```

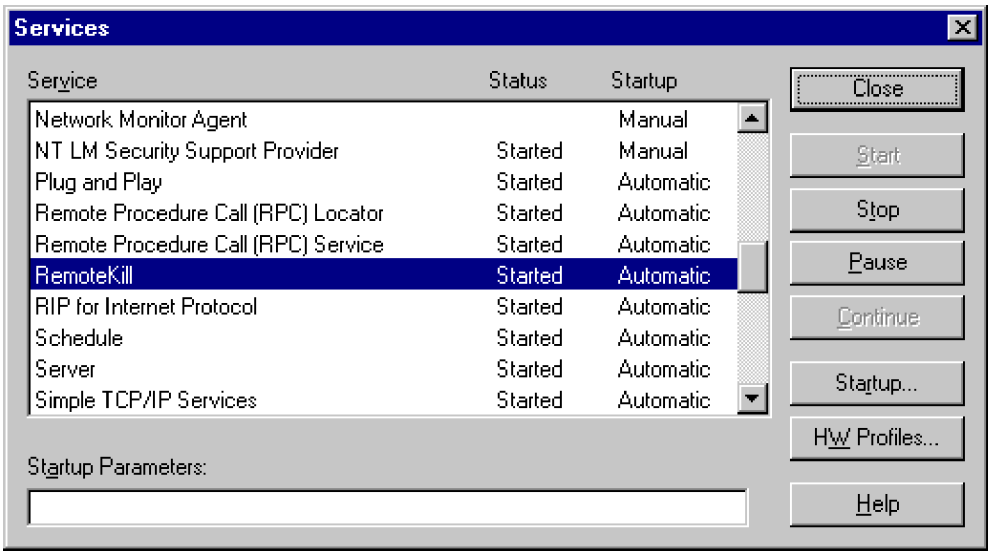


Remote Kill

Resource Kitin apuohjelma **Remote Kill** (**RKILLSRV.EXE**) on NT:n palvelu, joka mahdollistaa prosessien lopettamisen toisesta NT-koneesta.

Käytettävissä on sekä käyttöliittymä (**WRKILL.EXE**) että komentorivi (**RKILL.EXE**). Jotta tätä voidaan käyttää, käyttäjätunnuksen on oltava kohdekoneessa **Administrators**-ryhmän jäsen.

RKILLSRV.EXE voidaan käynnistää joko **INSTSRV.EXE**:llä tai graafisella **SRVINSTW.EXE**:llä.

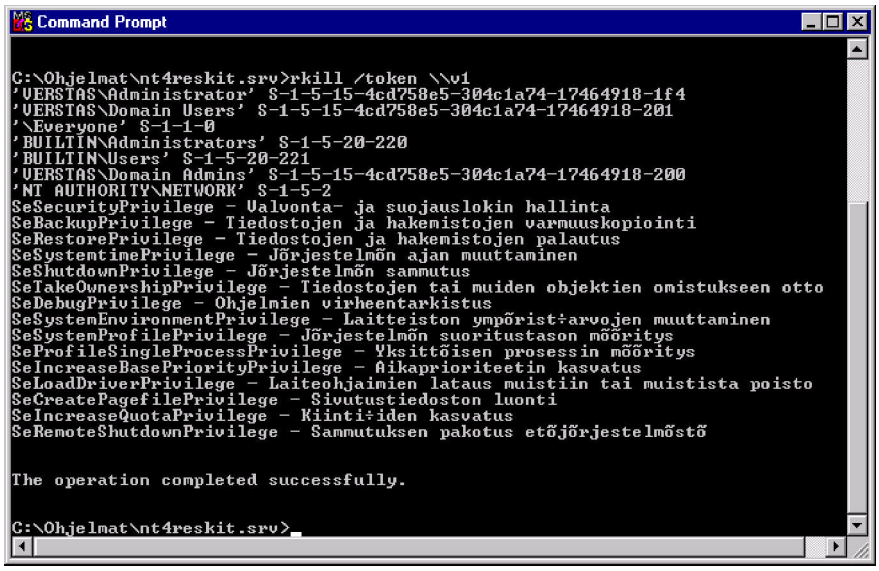


Palvelun asentamisen (tai komentorivillä käynnistämisen jälkeen) voit kokeilla **Rkill**-komentoa.

Komennolla

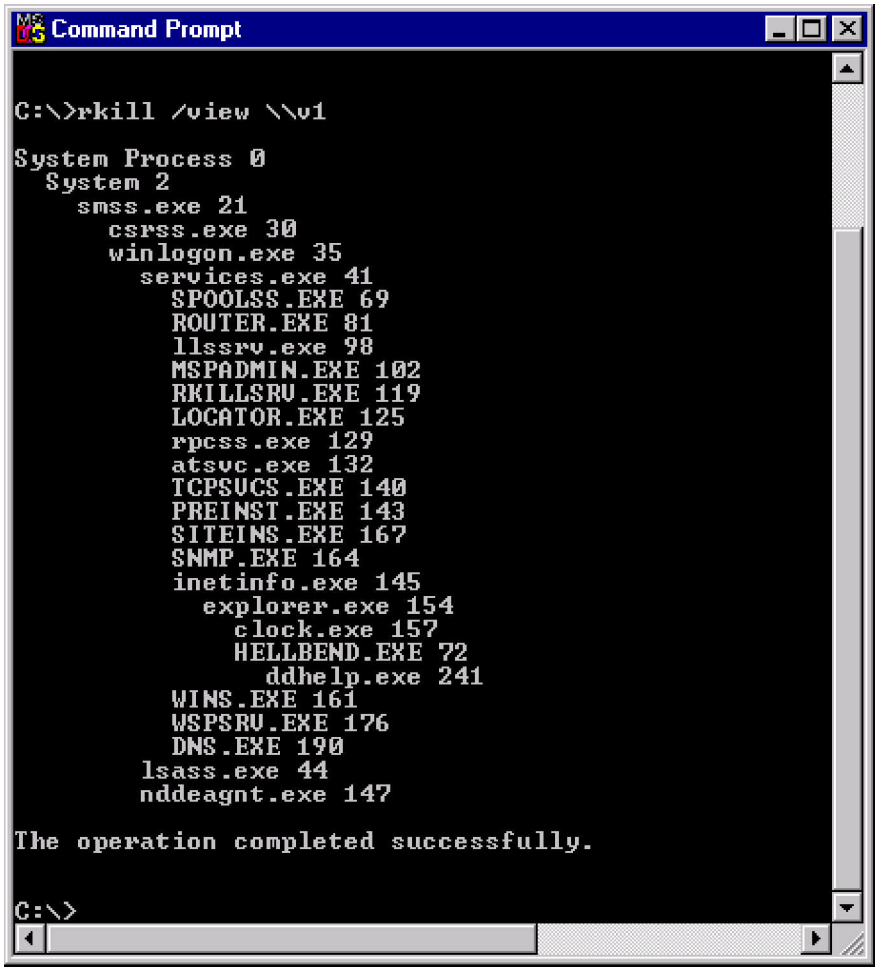
Rkill /token [NT-kone]

saat luettelon oikeuksistasi kyseisessä NT-koneessa. **SeProfileSingleProcessPrivilege**-oikeuden avulla voit tappaa prosesseja.



Prosessit näet komennolla

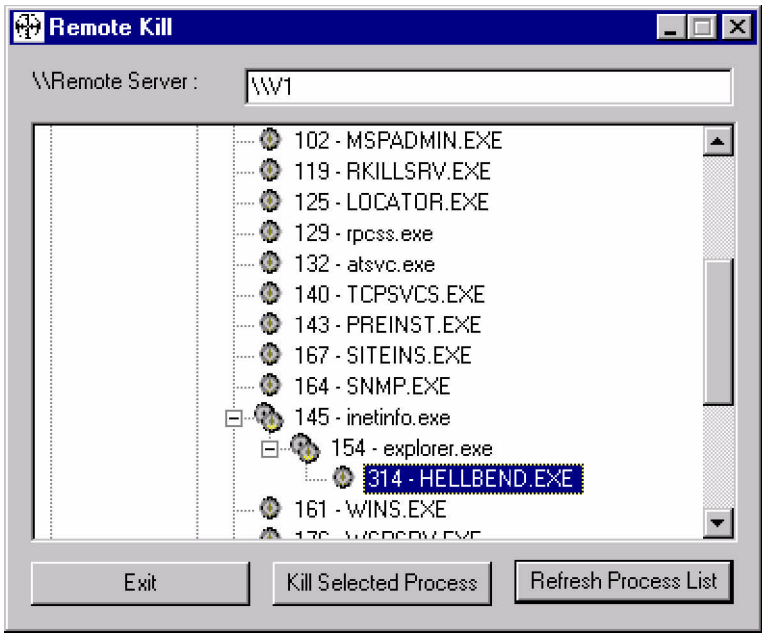
Rkill /view [NT-kone]



32-bittinen **HellBender**-peli näkyy omalla nimellään! Prosessi-id on **72**. Komento olisi siis esimerkin tapauksessa:

Rkill /kill \\V1 72

Toinen tapa on **Wrkill.exe**-ohjelma, jolla asiat voidaan hoitaa tyylikkäästi käyttöliittymän avulla.

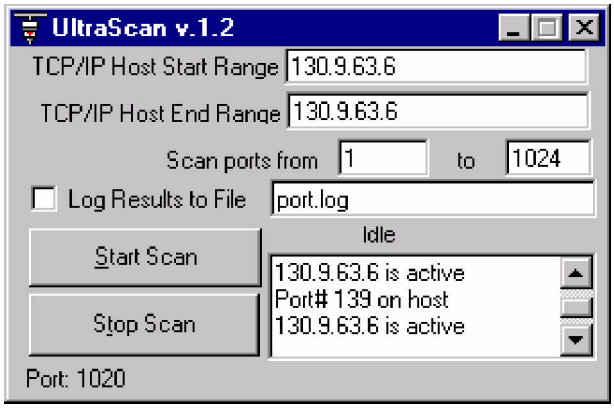


Valitse haluttu prosessi ja paina **Kill Selected Process**.

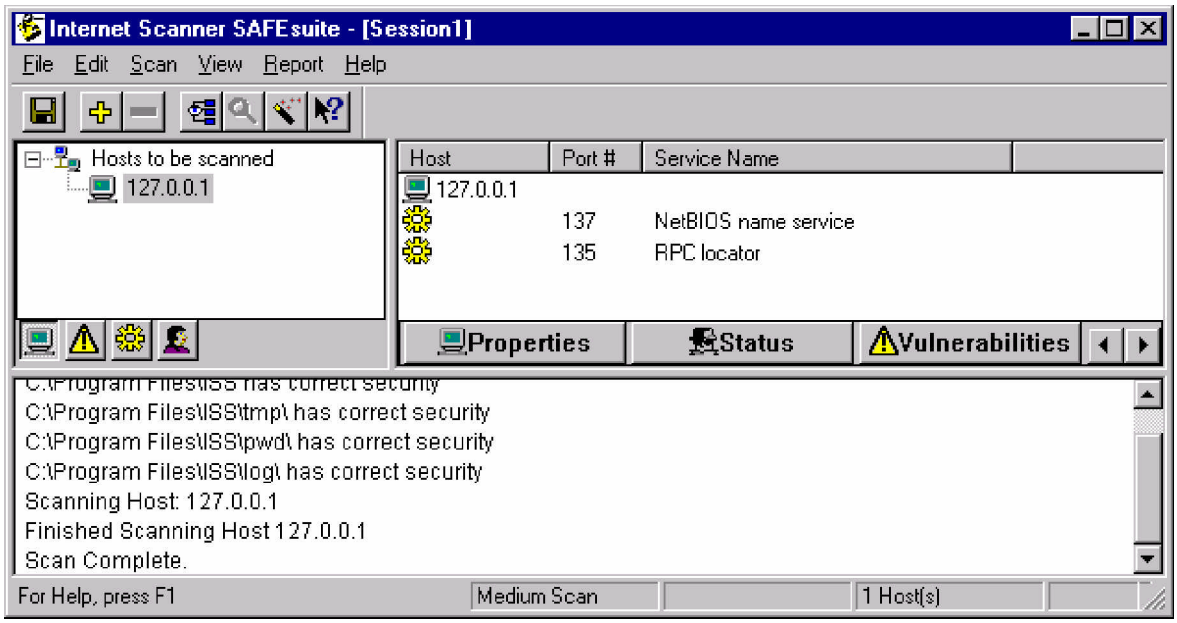
Porttien tutkijat

Jokainen TCP/IP-protokolliin liittyvä palvelu käyttää jotakin porttia. Porttien tutkijat (Port scanners) etsivät ne portit, jotka kuuntelevat, ja näin päästään käsiksi palveluihin.

Eräs porttien tutkimisohjelma on **UltraScan**. Shareware-version voi noutaa osoitteesta **http://www.x.gen.il.us/UltraScan**.



Toinen hieman laajempi on **Internet Scanner SAFEsuite**, jonka kokeiluversio löytyy osoitteesta **http://www.iss.net**. Se tutkii myös löytyvät palvelut sekä voi tallentaa lokin.



Puhelinyhteyksien tutkijat

Puhelinyhteyksien tutkijat (Dial-up scanners) etsivät käynnissä olevat modeemit. Jos ilmenee tarvetta modeemipalveluihin, kannattanee asentaa vaikkapa NT:n RAS (*Remote Access Service*) -palvelin tätä tarkoitusta varten. Jotkut käyttäjät saattavat preferoida omaan työasemaansa liitettyjä modeemeita, ja tällaiset ovat myös oivallisia takaovia hakkereil-

le. Resource Kitistä löytyy apuohjelmia RAS-palvelimien etsimiseksi verkosta.

Modeemien etsintäohjelmia organisaation aktiivisten modeemien etsimiseksi rakentelevat tietysti myös hakkerit ja krakkerit.

Eräs tällainen scanneri on **ToneLoc**, jonka tekijä *Minor Threat* joutui tekemisiin Yhdysvaltain eri viranomaistahojen kanssa (http://www.paranoia.com/~mthreat/story.html).

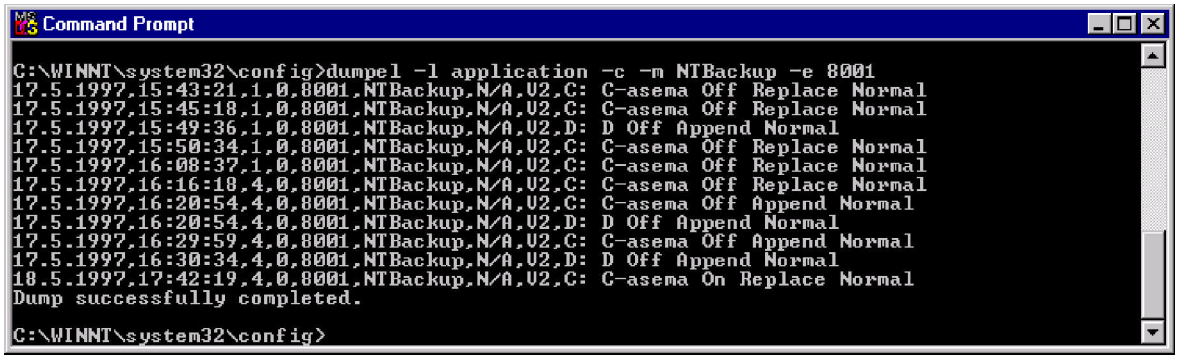
Tapahtumalokien analysointiohjelmat

Tapahtumalokien analysointiohjelmien (Event log analyzers) avulla voit viedä Event Viewerin lokit jatkokäsiteltäväksi esimerkiksi taulukkolaskentaohjelmaan, tietokantaan tai komentojonoon.

Resource Kitin mukana tulee **Dumpel**, jolla voit tehdä mukavasti dumppauksia minkä tahansa NT-koneen lokeista. Esimerkin komennolla

dumpel -l application -c -m NTBackup -e 8001

on tuotu näyttöön paikallisen NT-koneen tapahtumalokista **NTBackup**-ohjelman tapahtumat **8001**, jotka kertovat varmistuksen päättymisestä.



Suodatettu loki voidaan ohjata vaikkapa **findstr**-apuohjelmalle, ja **Errorlevel**-paluukoodin kautta voidaan käynnistää haluttuja toimintoja:

```
dumpel -l security -c -s V1 -f c:\temp\puppu.txt
findstr F:\DOOM2 c:\temp\puppu.txt
if errorlevel 1 goto loppu
...halutut toiminnot
```

Dumpel-ohjelman valitsimet ovat seuraavat:

-s <NT-kone>	Kohteena oleva NT-kone
-f <tdsto.txt>	Tulostus ohjataan tiedostoon nimeltä tdsto.txt
-l <loki>	Käsiteltävä loki: **system**, **application** tai **security**. Oletus on **application**
-m <lähde>	Lokin tapahtuman lähde (NTBackup, Rdr, Serial, El509x ...)
-e <id> <id>	Tapahtuman tunnus (id), maksimi 10 kappaletta
-r	Kaikki tapahtumat **paitsi** -e:llä mainitut
-t	Käytetään tabulaattoria erottimena.

Resource Kitin mukana tulee **Seagate Crystal Reports for NT 4.0**. Edellyttää rekisteröinnin ennen koekäyttöä!

SomarSoftin (**http://www.somar.com**) **DumpEVT** on myös erittäin käyttökelpoinen työkalu, ja nopea. Sen asetuksia voi muuttaa tarvittaessa IN-tiedoston kautta. Komentorivi on esimerkiksi

```
dumpevt /logfile=sec /computer=V1 /outfile=c:\temp\list.txt /all
```

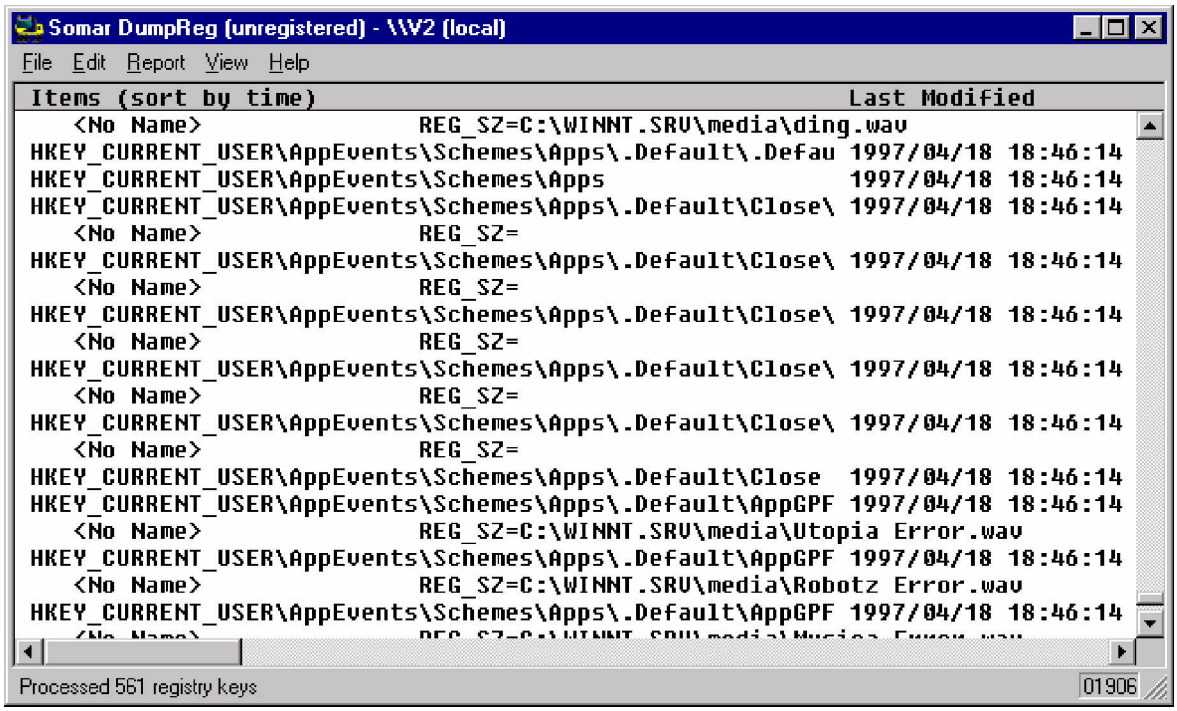
Yksi rivi tapahtumalokista näyttää tällaiselta:

```
SEC,27.5.1997  20:48:17,Security,560,8,3,VERSTAS\JKI,V1,Security;File;
F:\DOOM2\DOOM2.WAD;2844;0;54205;2154991104;SYSTEM;
NT AUTHORITY;(0x0;0x3E7);jki;VERSTAS;(0x0;0xD38A);
```

Rekisterien analysointiohjelmat

Rekisterien analysointiohjelmat (Registry analyzers) helpottavat rekisterien tutkimista. Niiden avulla voi mm. Tutkia sovellusten rekisteriin kirjoittamia asetuksia, tulostaa raportteja ja automatisoida tehtäviä.

Tällainen on esimerkiksi **SomarSoftin** (**http://www.somar.com**) **DumpReg**.



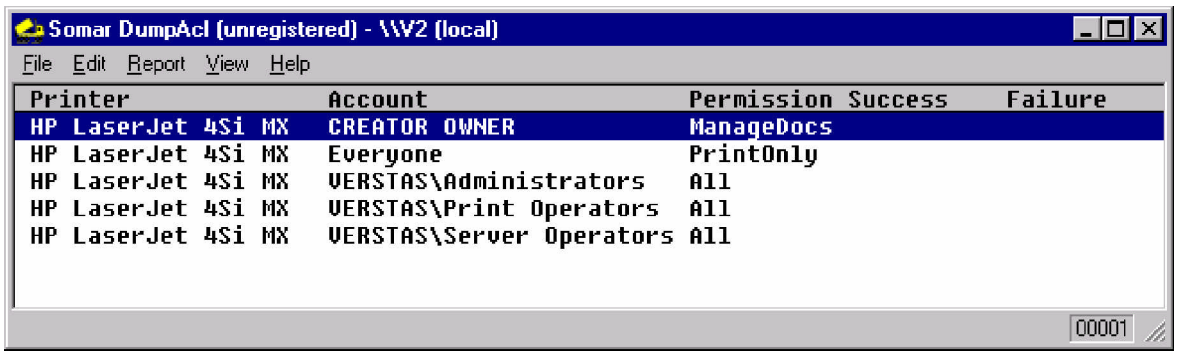
Käyttöoikeusluettelojen analysointiohjelmat

Käyttöoikeusluettelojen (*Access Control List*) analysointiohjelmat (Access control analyzers) mahdollistavat käyttöoikeuksien tarkastelemisen ymmärrettävämmässä muodossa kuin tavalliset Windows NT:n käyttöliittymän listaukset.

Windows NT:n oma komento **CACLS** toimii komentoriviltä ja mahdollistaa siten käyttöoikeuksien määrittelyn komentojonoista..

Näitä tulee myös Resource Kitin mukana, ja niitä on käsitelty aiemmin tässä luvussa.

SomarSoftin (**http://www.somar.com**) **DumpACL** on varmasti yksi suosituimmista käyttöoikeusluettelojen dumppausohjelmista.

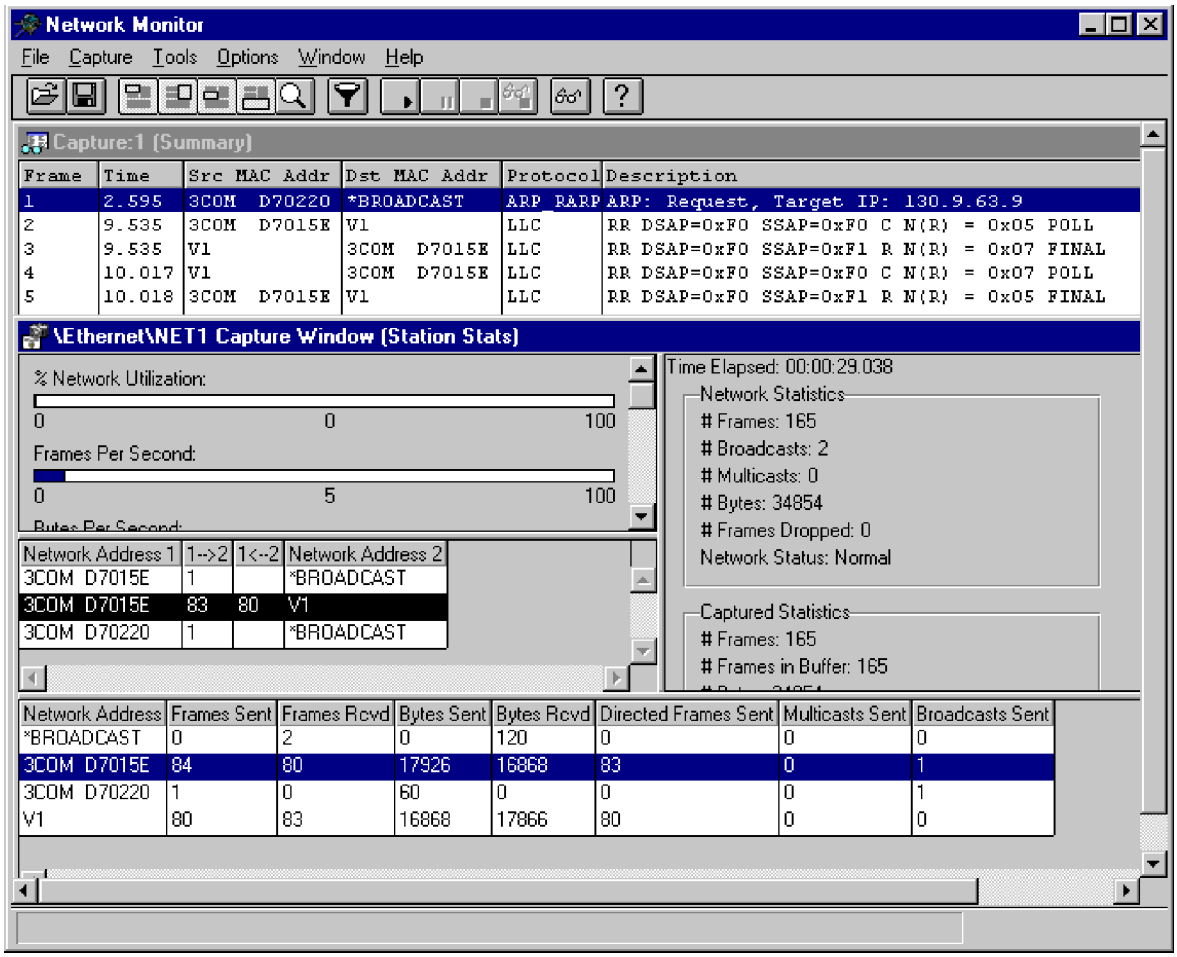


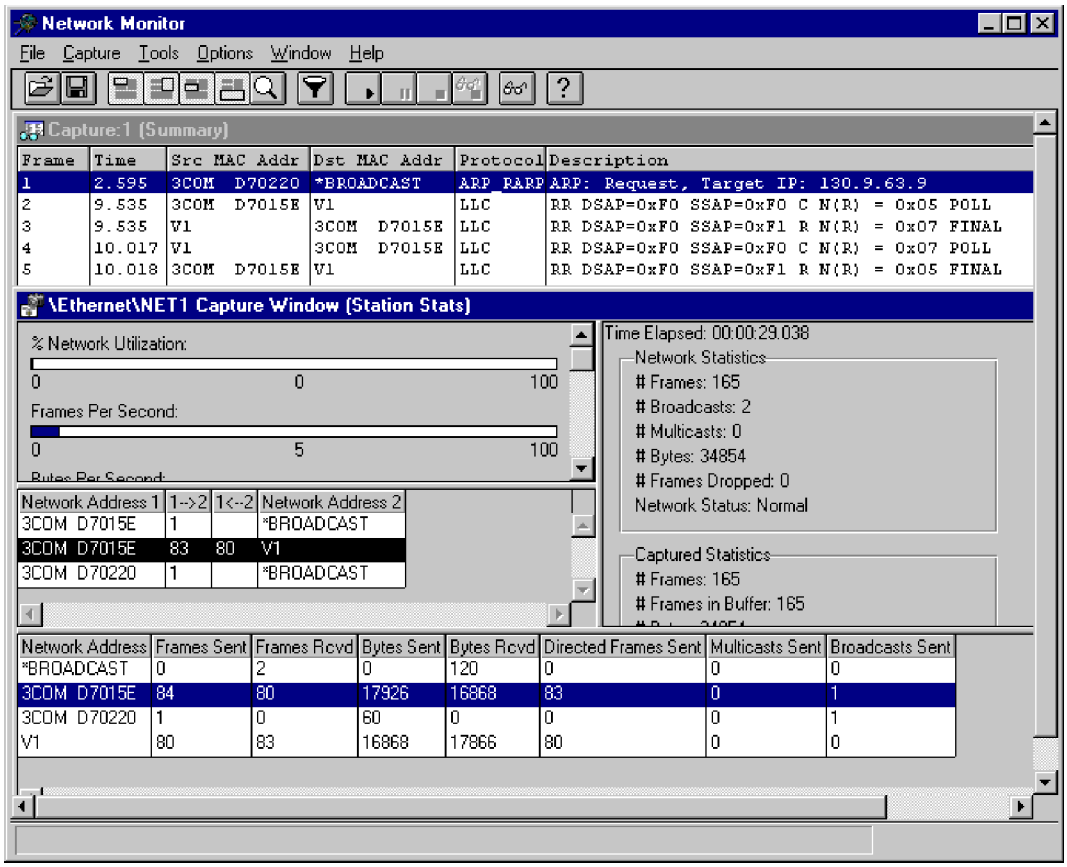
Protokolla-analysaattorit

Protokolla-analysaattorit ja pakettien tutkijat (Protocol analyzers, packet sniffers) mahdollistavat verkon liikenteen seuraamisen pakettitasolla. Tällöin voit seurata mitä todellisuudessa tapahtuu esimerkiksi palvelimen ja työaseman välillä.

Cinco Networksin NetXRay (**http://www.cinco.com**) toimii sekä Windows NT:ssä että Windows 95:ssä. Se edellyttää että verkkokortti toimii ns. valikoimattomassa tilassa (*Promiscuous mode*), jolloin voit seurata yhdestä pisteestä verkon liikennettä, olipa paketin kohde verkossa mikä hyvänsä.

Windows NT-palvelimen mukana tulee **Network Monitor**. Se voi seurata vain oman segmentin liikennettä, mutta on kuitenkin integroitu Microsoftin **Systems Management Serveriin** (SMS), jolla liikennettä voidaan seurata muualtakin.


Network Monitor
File Capture Tools Options Window Help
Capture:1 (Summary)
Frame Time Src MAC Addr Dst MAC Addr Protocol Description
1 2.595 3COM D70220 *BROADCAST ARP_RARP ARP: Request, Target IP: 130.9.63.9
2 9.535 3COM D7015E V1 LLC RR DSAP=0xF0 SSAP=0xF0 C N(R) = 0x05 POLL
3 9.535 V1 3COM D7015E LLC RR DSAP=0xF0 SSAP=0xF1 R N(R) = 0x07 FINAL
4 10.017 V1 3COM D7015E LLC RR DSAP=0xF0 SSAP=0xF0 C N(R) = 0x07 POLL
5 10.018 3COM D7015E V1 LLC RR DSAP=0xF0 SSAP=0xF1 R N(R) = 0x05 FINAL
\Ethernet\NET1 Capture Window (Station Stats)
% Network Utilization:
0 0 100
Frames Per Second:
0 5 100
Time Elapsed: 00:00:29.038
Network Statistics
Frames: 165
Broadcasts: 2
Multicasts: 0
Bytes: 34854
Frames Dropped: 0
Network Status: Normal
Captured Statistics
Frames: 165
Frames in Buffer: 165
Network Address 1 1-->2 1<--2 Network Address 2
3COM D7015E 1 *BROADCAST
3COM D7015E 83 80 V1
3COM D70220 1 *BROADCAST
Network Address Frames Sent Frames Rcvd Bytes Sent Bytes Rcvd Directed Frames Sent Multicasts Sent Broadcasts Sent
*BROADCAST 0 2 0 120 0 0 0
3COM D7015E 84 80 17926 16868 83 0 1
3COM D70220 1 0 60 0 0 0 1
V1 80 83 16868 17866 80 0 0



Salausmenetelmät

Salauksella tarkoitetaan tiedon muuntamista tietyn avainarvon avulla muotoon, jossa tietoja on vaikea (mieluiten mahdotonta) lukea. Salaus voidaan purkaa tietyn avaimen avulla. Salausta käytetään yleisesti suojaamaan kiintolevylle tallennettuja tietoja ja suojaamaan tiedonsiirtoa epävarmoja kommunikaatiokanavia pitkin.

Tyypillisiä salauskohteita ovat:

- Kirjautumisen aikana välitettävät salasanat
- Kirjautumispalvelimen kiintolevyllä säilytettävät salasanatiedostot (joiden avulla hyväksytään käyttäjän lähettämä salasana)

- Käynnistyslohkot ja tiedostotaulukot (joiden avulla kätketään levypartitioita ja tiedostojen sijaintia)
- Luottamukselliset tiedot, joita säilytetään varkauksille alttiilla kiintolevyillä
- Tietoliikenneyhteydet ja -istunnot
- Sähköiset kirjekuoret, joilla kätketään sähköpostiviestin sisältö ja suojataan sitä
- Sähköiset allekirjoitukset, joiden avulla voidaan tarkistaa viestejä ja liiketapahtumia
- Sertifiointipalvelut, joiden avulla voidaan hyväksyä julkisten verkkojen käyttäjiä.

Lisätietoja:

- http://www.rsa.com
- http://www.commerce.net
- http://www.cybercash.com
- http://www.digicash.com
- http://www.fv.com
- http://www.mondex.com
- http://www.cylink.com
- http://www.verisign.com
- http://www.usps.gov
- http://www.security.com
- http://www.cert.org
- http://www.gocsi.com
- http://www.uhsa.uh.edu/issa/
- http://www.ncsa.com

Salausprosessiin kuuluu tiedon salaaminen (*encryption*) ja salauksen purkaminen (*decryption*). Nämä pohjaavat kahteen tärkeään asiaan: avaimeen ja algoritmiin (salausmekanismiin). Seuraavaksi kuvaillaan joitakin mm. Windows NT -ympäristössä käytössä olevia menetelmiä.

Yksisuuntaiset funktiot ja salaovet

Yksi perussalausmenetelmistä on **yksisuuntainen funktio** (*one-way function*, OWF). Tehokkuus- ja turvallisuussyistä funktio on helppo toteuttaa yhteen suuntaan eli salattaessa, mutta vaikea toteuttaa käänteisenä, eli purettaessa salausta. Näitä tapahtumia kuvataan termeillä *forward function* (salaus) ja *reverse function* (käänteisfunktio eli salauksen purkaminen).

Funktio, jolla salaaminen tehdään, on tavallisesti helppo toteutaa ja siihen voi kulua vain pari sekuntia, mutta käänteinen salauksen purkufunktio on vaikea ja siihen voi kulua vuosia käytetystä algoritmista ja avaimen koosta riippuen. Windows NT käyttää OWF:ää salasanojen salaukseen, koska prosessi on nopea, mutta salausta on vaikea purkaa. Salasanan salausta ei tarvitse koskaan purkaa, koska salauksen jälkeen verrataan keskenään salakirjoitettuja salasanoja. Koska yksisuuntaisia funktioita on vaikea ajaa toiseen suuntaan, ne estävät tehokkaasti mahdollisia tunkeutujia purkamasta salasanojen suojausta.

Yksisuuntainen salaovifunktio (*trap door one-way*) on funktio, jolla toteutetun salauksen purkaminen on helppoa, koska sitä varten on luotu avain (salaovi). RSA:n julkisen avaimen salausjärjestelmät perustuvat yksisuuntaisiin salaovifunktioihin:

- Salaus toteutetaan julkisella avaimella, jonka avulla voidaan salata viestejä tai todentaa allekirjoitus
- Yksityinen avain on tarvittava käänteinen salaovifunktio (*reverse trap door function*), jonka avulla voidaan purkaa yksityisten viestien salaus ja luoda sähköisiä allekirjoituksia.

Sifferit ja Hash-algoritmit

Salainen avain -kryptauksessa käytetään tietojen salaukseen yhtä ainoaa avainta, ei kahta avainta (kuten julkiseen ja yksityiseen avaimeen perustuvassa salauksessa). Salakirjoitus- eli sifferimenetelmiä ovat **block**- ja **stream ciphers** sekä **hash**-funktiot.

- **Lohkon salakirjoitus** (*Block cipher*) on tavallisen tekstin muuntaminen salakirjoitukseksi salaisen avaimen avulla. Salakirjoitus voidaan sitten purkaa käyttämällä salaista avainta

käänteisen muunnoksen tekemiseen. Tavallinen teksti muunnetaan 64 bitin lohkoiksi. **Iterated block cipher** -menetelmä koostuu useista **block ciphereistä**, joissa alkuperäistä tekstiä muunnetaan aliavainten (*subkeys*) avulla, jotka saadaan käyttäjän antamasta alkuperäisestä salaisesta avaimesta. Idea on se, että toistojen määrä lisää turvallisuutta.

- **Tietovirran salakirjoitus** (*Stream cipher*) toimii bittitasolla eikä tietolohkojen tasolla, ja se on tavallisesti nopeampi kuin **block cipher**. Tärkeintä tässä on, että saman avaimen käyttäminen samaan tekstiin kahdesti saa aikaan kaksi erilaista salakirjoitettua tekstiä. Block cipher tuottaa saman salakirjoitustekstin aina, kun samaa avainta käytetään.

Tietoa voidaan salauksen yhteydessä pakata, mistä voi olla hyötyä, koska tällöin poistuu tiedon ylimäärää (*redundancy*). Pakatussa tiedostossa on tasainen merkkijakauma, mikä vaikeuttaa joidenkin purkumenetelmien käyttöä. Huomaa, että tieto täytyy pakata **ennen** salausta, ei sen jälkeen.

Data Encryption Standard (DES)

DES on Yhdysvaltain hallituksen virallinen salakirjoitusstandardi. Se on **symmetrinen lohkon salausjärjestelmä** (*block cipher symmetric*), jonka on alunperin kehittänyt IBM. DES:iä on sen käyttöönoton jälkeen tutkittu tarkoin ja se on laajalti käytössä ympäri maailman. Sitä käytetään usein myös yhden käyttäjän ympäristöissä kiintolevyllä säilytettävien tietojen salaukseen. Microsoft käyttää DES:iä viestien salaukseen **Microsoft Exchangessa** ja **Windows NT** -palvelimissa käyttäjän kirjautumistarkistusten salauksessa.

DES:in lohkokoko on 64 bittiä ja siinä käytetään tietojen salaukseen 56-bittistä avainta. Alkuperäisessä versiossa määritettiin laitteistokokoonpano. DES on osoittautunut hyvin vaikeaksi murtaa: avainavaruuden kattavaksi kartoittamiseksi on tehty *raakaa voimaa* käyttäviä yrityksiä, mutta tällaiset menetelmät soveltuvat tavallisesti huonosti krakkerien käyttöön. Saatavilla on myös kolmoiskryptattu DES, joka on huomattavasti turvallisempi kuin tavallinen DES.

DES:in turvallisessa käytössä salasanoja pitäisi vaihtaa usein. Jos DES-avain täytyy vaihtaa jonkun kanssa esimerkiksi sähköpostin kautta, käytä lisäksi julkisen avaimen salausmenetelmiä DES-avaimen salauk-

seen vastaanottajan julkisella avaimella, jolloin vastaanottaja voi purkaa salauksen omalla yksityisellä avaimellaan.

Kun DES:iä käytetään kiintolevyillä olevien tietojen salaukseen, ei ole kovinkaan käytännöllistä vaihtaa DES-avaimia usein. On myös mahdollista, että kauan sitten tietojen salaukseen käytetyt avaimet unohtuvat. Nämä ongelmat voi ratkaista tekemällä käytetyistä DES-avaimista luettelon, joka sitten salataan DES-pääavaimella.

DES:in mahdolliseksi korvaamiseksi on kehitetty useita salakirjoitusalgoritmejä, mutta joidenkin niistä on havaittu olevan alttiita hyökkäyksille. Seuraavassa mainitaan muutama onnistuneimmista menetelmistä.

IDEA

IDEA (*International Data Encryption Algorithm*) on 64 bitin lohkoja käyttävä salakirjoitusmenetelmä, jossa käytetään 128-bittistä avainta ja kahdeksaa laskukertaa. IDEA on tarkoitettu sekä ohjelmisto- että laitteistosovelluksille, ja sen nopeus ohjelmistosalauksessa on suunnilleen samaa luokkaa kuin DES:in. IDEA:n kehitystyön tärkein tavoite oli suojautua tietyntyyppisiltä hyökkäyksiltä, joita DES aiemmin kohtasi. IDEAa pidetään yleensä turvallisena.

SAFER

SAFER (*Secure And Fast Encryption Routine*) -lohkosalakirjoitus-menetelmä kehitettiin vuonna 1993 Cylink Corporationille. Siinä käytetään 64 bitin lohkokokoa, enintään 64-bittisiä avaimia ja enintään kymmentä laskukertaa. Salakirjoitus on tarkoitettu käytettäväksi älykorteissa, joissa prosessointiteho on rajallinen.

Blowfish

Tämä salakirjoitusmenetelmä käyttää 64 bitin lohkoja ja enintään 4 448 bitin avaimia. Avaimesta luodaan useita **aliavainsarjoja**. Menetelmä kehitettiin 32-bittisille tietokoneille, mutta jotkin hyökkäykset sitä

vastaan onnistuivat hyvin. Menetelmää pidetään siitä huolimatta yhä turvallisena, koska käytetyt hyökkäystyypit olivat kuitenkin käytännön kannalta hankalia.

Skipjack

Tämä algoritmi kuuluu Yhdysvaltain hallituksen Capstone-projektiin, ja sitä käytetään **Clipper**-sirussa. Sen on kehittänyt **National Security Agency** (NSA). Skipjackissa käytetään 80-bittistä avainta ja 32 laskentakierrosta (kun DES:issä käytetään 56-bittistä avainta ja 16 laskentakertaa). Skipjack on saatavilla vain laitteistona Yhdysvaltain hallituksen valtuuttamilta valmistajilta, ja sen tiedot ovat salaisia.

RC-algoritmit

RSA Data Securityn Ron Rivest on kehittänyt seuraavat algoritmit DES:iä korvaaviksi vaihtoehdoiksi. Niiden kaikkien avaimen pituus vaihtelee, jolloin sitä voidaan muuttaa halutun turvallisuustason mukaan. Kaikki kolme ovat ohjelmistotasolla nopeampia kuin DES. Ennen kaikkea kuitenkin RC2:n ja RC4:n etuna on se, että niillä on Yhdysvaltain hallituksen erityislupa, jolloin vientiluvan saaminen Yhdysvalloissa on helpompaa, jos avaimen koko on rajattu 40 bittiin. RC2 ja RC4 ovat laajalti käytössä niissä ohjelmistotaloissa, joiden tuotteita myydään Yhdysvaltain ulkopuolelle, koska DES ei juuri koskaan saa vientilupaa.

- **RC2**-lohkosalakirjoitusmenetelmä (64-bittinen), joka on kaksi kolme kertaa ohjelmistotasolla nopeampi kuin DES. Algoritmi on salainen ja RSA Data Securityn omaisuutta. RC2:ta voidaan käyttää samoissa toimintatiloissa kuin DES:iä. RC2:lle on helpompi saada vientilupa, mutta sen avaimen (samoin kuin RC4:n) koko täytyy viennissä rajoittaa 40 bittiin (56 bittiä sallitaan Yhdysvaltalaisten yritysten ulkomaisille tytäryhtiöille ja ulkomaantoimipisteille). Lisäksi voidaan käyttää ylimääräistä merkkijonoa, *saltia* (40 80 bittiä pitkä) tekemään tyhjäksi sellaisten hyökkääjien aikeet, jotka yrittävät luoda taulukon mahdollisista salauksista. Salt lisätään salausavaimeen ja viesti salataan tällä pidennetyllä avaimella, minkä jälkeen salt lähetetään ja sen salaus puretaan yhdessä viestin mukana.

- **RC4** on **stream cipher**, jonka avaimen pituus vaihtelee ja joka toimii bittitasolla. Algoritmi on salainen ja RSA Data Securityn omaisuutta. Riippumattomat tutkijat ovat kuitenkin tutkineet sitä, ja sitä pidetään turvallisena.

- **RC5** on nopea lohkosalakirjoitusmenetelmä, jonka parametrit voidaan määrittää itse halutun turvatason ja tehokkuuden mukaan. Lohkokoko (32, 64 tai 128 bittiä), avaimen koko (0 2 048 bittiä) ja laskentakertojen määrä (0 255 kierrosta) voidaan määrittää. RSA:n mukaan RC5:n turvallisuus perustuu tiedoista riippuvien toistojen (*Data-dependent rotations*) laajaan käyttöön ja eri menetelmien sekoittamiseen, mikä auttaa erityisesti vastustamaan ns. *differentiaalista* ja *lineaarista* salausanalyysia.

Hash-algoritmi

Hash-funktion avulla luodaan sanoman lyhennelmä (*digest*), jota voidaan käyttää sähköisissä allekirjoitussovelluksissa. Lyhennelmä salakirjoitetaan yksityisellä avaimella. Kun vastaanottaja saa viestin, myös hän käsittelee viestin Hash-funktiolla ja vertaa saamaansa lyhennelmää lähetettyyn lyhennelmään, jonka salaus on purettu. Jos lyhennelmät ovat samanlaiset, viestiä ei ole muutettu.

Ron Ricest on luonut kolme laajalti käytössä olevaa hash-funktiota: **MD2**, **MD4** ja **MD5**. Kaikki kolme ottavat satunnaisen pituisen viestin ja tuottavat siitä 128-bittisen lyhennelmän:

- **MD2**-algoritmi kehitettiin vuonna 1989 ja se suunniteltiin 8-bittisille tietokoneille (MD4 ja MD5 on tarkoitettu 32-bittisille tietokoneille). Ensiksi viestiin lisätään tyhjiä merkkejä, jotta sen bittipituus saadaan jaolliseksi luvulla 16. Sitten viestiin lisätään 16-bittinen tarkistussumma, ja tästä viestistä lasketaan **hash**-arvo.

- **MD4**-algoritmi kehitettiin vuonna 1990. Viestiä on täytetty, jotta sen bittipituus + 448 olisi jaollinen luvulla 512. Viestin alkuperäisen pituuden 64-bittinen binaarimuoto liitetään viestin perään. Hash luodaan kolmella käsittelykierroksella. RSA:n mukaan *kehitettiin nopeasti onnistuneita hyökkäyksiä MD4:ään,*

josta puuttui ensimmäinen tai viimeinen käsittelykierros ja *ristiriitoja MD4:n täydellisen version kanssa löytyy tavallisella PC:llä alle minuutissa. Ilmiselvästi MD4:ää voidaan pitää murrettuna.*

- **MD5**-algoritmi kehitettiin vuonna 1991. Se on MD4:n turvallisempi versio, jossa käytetään neljää käsittelykertaa.

Microsoft CryptoAPI

Microsoft kehitti **Cryptographic API**:n (*CryptoAPI*), jotta ohjelmoijien olisi helpompi kehittää salausta ja sähköisiä allekirjoituksia sisältäviä sovelluksia sekä samalla pystyä turvaamaan käyttäjän salainen yksityinen avain. CryptoAPI koostuu moduuleista, joita sanotaan salauspalveluntarjoajiksi (*Cryptographic Service Provides*, CSP). Kukin moduuli hoitaa jotakin tiettyä salauspalvelua, jota kehittäjät voivat käyttää. Yksi CSP (*Microsoft RSA Base Provider*) liittyy Windows NT-käyttöjärjestelmään. CryptoAPI tekee helpoksi turvaominaisuuksien käytön esimerkiksi seuraavanlaisissa tehtävissä ja sovelluksissa:

- Oletuskäyttäjän avainvarannon luominen, julkisen ja yksityisen avainparin luominen allekirjoituksia varten ja avainten vaihtaminen
- Sovellukset, joissa salataan tiedostoja ja puretaan niiden salausta
- Sovellukset, joilla salataan, allekirjoitetaan ja tunnistetaan viestejä ja tiedostoja.

Microsoft CryptoAPI on saatavilla Microsoft Internet Exploreriin, Windows NT 4.0:aan ja Windows 95:een. Muut ohjelmistotuottajat käyttävät CryptoAPI:a kehittäessään sovelluksia, joissa Windows NT:tä käytetään sähköisen kaupan alustana. API:n avulla voidaan myös kirjoittaa valtuuteen perustuvia varmennuksia (*token-based authentication*) ja turvasovelluksia sekä organisaation kattava julkisten avainten järjestelmä salaus- ja allekirjoitustarkoituksiin. CryptoAPI tekee salakirjoituksesta helpommin käytettävän.

Turvallinen tiedonsiirto

Tiedonsiirron suojaamisessa voidaan käyttää seuraavia menetelmiä:

- Varaudu ennalta salakuuntelijoihin, linjankuunteluun ja istuntojen kaappaamiseen
- Turvaa fyysisesti alueet, joilla on tiedonsiirtokaapeleita
- Seuraa ulkopuolisten asentajien ja konsulttien toimia. He voivat salakuunnella sisäistä verkkoa
- Käytä optisia kaapeleita luottamuksellisen tiedon siirtämiseen ja estämään nuuskijoiden kaappaamien pakettien korvaaminen verkossa
- Jos otat yhteyttä muihin toimipaikkoihin internetin kautta, suojaa yhteys salauslaitteilla, jotka ylläpitävät automaattisesti toimipaikkojen välisiä linkkejä ja salaavat kaiken siirrettävän tiedon
- Modeemiyhteyksillä internetin yli voit käyttää PPTP-protokollaa.

Protokolla	Kuvaus	Liittymät
S-HTTP	WWW-liikenteen suojaaminen	SSL, PCT
SSL	Suojaa SSL:ää käyttävien sovellusten liikenteen; pitkät avaimet voivat aiheuttaa suorituskykyongelmia	S-HTTP, PCT
PCT	Suojaa WWW-maksuliikenteen; Microsoftin tukee; laajentaa SSL:n suojauksia	SSL, S-HTTP
SET	Suojaa palvelu- ja sovellustasolla Internet-maksuliikenteen	SSL, S-HTTP
IPsec	Suojaa sovellustasolla TCP/IP-liikenteen; edellyttää laitteiston tukea	S/MIME
SPKM/GSS	Sovellustason suojaus; Kerberos-yhteensopiva	
S/MIME	Suojaa sähköpostiliikenteen, edellyttää sovellustason tukea	IPsec

Microsoft Internet Security Framework

Microsoft Internet Security Framework on kokoelma julkisiin avaimiin ja salasanaturvaan perustuvia tiedonsuojausmenetelmiä, joiden avulla voidaan välittää informaatiota julkisissa verkoissa, valvoa pääsyä ulkopuolisista verkoista sisäisiin verkkoihin ja toteuttaa sähköistä kaupankäyntiä internetin välityksellä.

Microsoft Internet Security Framework on rakennettu CryptoAPI:n pohjalta. CryptoAPI:n päälle on rakennettu seuraavat turvallisuusominaisuudet ja -mekanismit:

- Turvatut kanavat yksityiseen kommunikaatioon SSL:n (versiot 2.0 ja 3.0) ja PCT:n avulla
- Sertifikaattipohjainen oikeuksien tarkistaminen

- Authenticode-menetelmä, jonka avulla voidaan varmistaa, että noudettua koodia ei ole muuteltu ja että koodilla on tunnettu julkaisija
- SET-protokolla turvallisiin luottokorttitapahtumiin
- Sertifikaattipalvelin, jolla voidaan myöntää ja peruuttaa sertifikaatteja
- **Microsoft Wallet**, johon voidaan tallentaa henkilökohtaisia turvatietoja kuten esimerkiksi avaimia, sertifikaatteja ja luottokorttitietoja
- **Personal Information Exchange** (PEX), jonka avulla henkilökohtaisia turvatietoja voidaan siirtää koneiden ja alustojen välillä (PIX sen sijaan on Ciscon palomuurituote Private Internet Exchange)
- Salasanapohjainen käyttäjäntunnistus
- Käytönvalvonta joko salasanoilla tai sertifikaateilla
- Salasanoihin perustuva jaettu oikeuksien tarkistusmenetelmä, sisältää myös integroinnin internetiin. Tämä menetelmä mahdollistaa välitetyn (*pass-through*) käyttäjäntunnistuksen ja salasanan suojauksen, jaetun oikeuksien tarkistamisen sekä liittymän Windows NT -käyttöjärjestelmän turvaominaisuuksiin.

Tunnistaminen, oikeuksien tarkistaminen ja oikeuksien myöntäminen hoidetaan julkiseen avaimeen ja salasanoihin perustuvilla menetelmillä.

Microsoftin Wallet, asiakkaan oikeuksien tarkistaminen, jaettu oikeuksien tarkistaminen, suojatun kanavan protokollat, CryptoAPI, Authenticode ja SET tulevat Microsoft Internet Explorerin kautta saataville Windows NT-, Windows 95-, Windows 3.x-, Macintosh- ja UNIX-ympäristöihin. Microsoft on myös Metrowerksin kanssa kehittämässä Authenticode-menetelmää Macintoshille.

Seuraavat ovat CryptoAPI:n osia:

- **Cryptographic Service Providers** (CSP:t) - salauspalveluntarjoajat ovat valinnaisia ohjelmistomoduuleja, esimerkiksi Microsoftin RSA-salakirjoitus tai jokin laitteisto (BBN SafeKeyper)

- **Cryptographic Primitives** - näiden avulla ohjelmoijat voivat valita salauspalveluntarjoajia, luoda ja tallentaa julkisia avaimia, salata ja purkaa tietoja, allekirjoittaa ohjelmansa sähköisesti ja varmistaa muiden allekirjoituksia

- **Cerfiticate Functions** - sertifikaattifunktioita ovat sertifikaattien luontipyyntöjen tekemiseen, sertifikaattien tallentamiseen ja noutamiseen sekä sertifikaattien jäsentämiseen liittyvät funktiot

- **High-level Cryptographic Calls** - näissä suljetaan useita salausalkeisfunktioita yhdeksi yksittäiseksi kutsuksi. Kehittäjä voi esimerkiksi salata tietoa ja purkaa salauksen, allekirjoittaa koodia ja varmistaa allekirjoituksia yksittäisellä funktiolla.

Seuraavat ylätason turvauspalvelut käyttävät CryptoAPI:a esimerkiksi yksityiseen tiedonsiirtoon, oikeuksien tarkistamiseen, liiketapahtumien turvaamiseen, sähköisen rahan hallintaan ja käyttöoikeuksien valvontaan.

Wallet

Wallet (lompakko) on sähkörahakomponentti, jolla on seuraavia ominaisuuksia:

- Se sijaitsee käyttäjän tietokoneella tai jollain muulla laitteella, esimerkiksi älykortilla

- Siihen tallennetaan yksityisiä turvatietoja, esimerkiksi yksityisiä avaimia, luottokorttinumeroita ja sertifikaatteja

- Se voidaan siirtää paikasta toiseen Personal Information Exchange (PFX) -protokollaa käyttämällä

- Sen käyttöoikeutta valvotaan.

Personal Information Exchange

Personal Information Exchange (PFX) -protokolla mahdollistaa luottamuksellisten tietojen siirtämisen yhdestä ympäristöstä tai alustalta toiselle. Käyttäjä voi esimerkiksi säilyttää sertifikaatti- ja avaintietoja toimistonsa PC:llä, mutta haluaa viedä tiedot myös kotona olevalle Macintoshille. Käyttäjä voi PFX-protokollan avulla siirtää turvallisesti henkilökohtaisia tietoja yhdestä tietokonejärjestelmästä toiseen.

Authenticode

Authenticode ratkaisee yhden suuren ongelman - kuinka käyttäjä voi luottaa siihen, että internetissä julkaistu koodi on aitoa. Authenticode on tapa allekirjoittaa koodi siten, että käyttäjä tietää internetistä hankkimansa ohjelmien olevan laillisia. Authenticode tarjoaa:

- Varmuuden - käyttäjä tietää, kuka on julkaissut koodin
- Eheyttä, eli tiedon siitä, että koodia ei ole muutettu sen julkaisemisen jälkeen
- Laillisen ja turvallisen tavan siirtää ohjelmia internetin kautta.

Jotta sovelluksen tekijä voisi allekirjoittaa koodin, hänen täytyy hankkia sertifikaatti joltain sertifikaatin myöntäjältä. Tekijä salakirjoittaa sertifikaattinsa yksityisellä avaimellaan koodiin, jolloin syntyy yksilöllinen allekirjoitus. Koodin aitous voidaan sitten todistaa käyttämällä menetelmiä, joilla sähköinen allekirjoitus varmistetaan. Näiden menetelmien avulla on mahdollista osoittaa, onko sovellus alkuperäinen, onko se väärennös tai onko joku muuttanut sitä.

Secure Sockets Layer

Jos kyseessä on liiketoiminta tai muuten luottamukselliset tiedot, tarvitaan WWW-selaimen käytössä suojattuja yhteyksiä. **Secure Sockets Layer** (SSL) on suojatutn kanavan turvallisuutta tarjoava protokolla. SSL:n avulla asiakas ja palvelin sopivat kättelemällä turvallisuustasosta, jota ne haluavat käyttää istunnon aikana. Oikeuksien tarkistaminen tapahtuu suojatulla kanavalla ja kaikki istunnon aikana välitettävä tieto

salakirjoitetaan. SSL:n ensimmäisiä versioita ei pidetä riittävän vahvoina takaamaan luottamuksellisen tiedon turvaamista.

Secure Hypertext Transfer Protocol

Toinen standardi sähköiseen turvaan on **Secure Hypertext Transfer Protocol** (**S-HTTP**). Se on sovellustason protokolla, joka voi esimerkiksi turvata tiettyjä dokumenttien osia. Se tunnistaa käyttäjät sähköisten allekirjoitusten avulla.

Personal Communications Technology

Microsoft Internet Security Framework tukee SSL-versioita 2.0 ja 3.0 sekä Personal Communications Technologyn (PCT) versiota 1.0. Siihen tulee tuki myös **Transport Layer Security Protocolille** (TLS), jota standardisointikomitea IETF on käsittelemässä. Tämän protokollan avulla voidaan käyttää sekä SSL:ää että PCT:tä. **PCT 1.0** on samantapainen kuin Secure Sockets Layer (SSL) 2.0, mutta edistyneempi oikeuksien tarkistamisen ja protokollan tehokkuuden kannalta. Koska PCT:ssä erotetaan oikeuksien tarkistaminen tiedon salaamisesta, sovellukset voivat käyttää tehokkaampia salausmenetelmiä kuin Yhdysvaltain vientirajoitusten mukaista 40-bittistä avainta. Microsoftin PCT-sovellus on yhteensopiva SSL:n aiempien versioiden kanssa.

SSL:n versio 3.0 tarjoaa oikeuksien tarkistamisominaisuuden sekä asiakkaalle että palvelimelle, jolloin kumpi tahansa voi pyytää oikeuksien tarkistamista toiselta. Oikeuksien tarkistamisen avulla käyttäjät voivat todeta palvelimien identiteetin ja palvelimet voivat todeta asiakasohjelmien identiteetin. Tähän tarvitaan sertifiointipalvelua.

Secure Electronic Transaction

Jotta kauppiaat voisivat turvallisesti kerätä ja käsitellä internet-asiakkaiden maksuja, tarvitaan turvaprotokolla, jota tukevat suurimmat luottokorttiyhtiöt ja ohjelmistotalot. Microsoft, IBM, Netscape, GTE, Visa ja MasterCard kehittävät tähän tarkoitukseen **Secure Electronic Transaction** (SET) -protokollaa.

SET:in tarkoituksena on turvata luottokorttitapahtumat tarkistamalla kortinomistajien, kauppiaiden ja pankkien oikeudet ja säilyttämällä maksutiedot salaisina. SET:issä käytetään sähköisiä allekirjoituksia asiakkaan, kauppiaan ja pankin tunnistamiseen. Siinä käytetään myös **monen osapuolen sanomia** (*multiparty messages*), joiden avulla tietoja voidaan salakirjoittaa ja lähettää suoraan pankeille. Näin luottokorttinumerot eivät päädy vääriin käsiin. Lisäksi tarvitaan luottokorttien käsittelyjärjestelmään vielä yhteys, jota ollaan juuri kehittämässä.

SET:in ja muiden maksuprotokollien yläpuolella tulee olemaan neuvottelukerros. Tämän kerroksen määritteleminen kuuluu **Joint Electronic Payment Initiative** -projektille (JEPI), johon Microsoft kuuluu. JEPI-projektissa tutkitaan menetelmiä, joiden avulla voidaan toteuttaa neuvottelukerros useiden maksumenetelmien, protokollien ja kuljetusprotokollien päälle. Maksumenetelmiä ovat esimerkiksi luottokortit, rahakortit, sähköinen raha ja shekit. Maksuprotokollat (esimerkiksi SET) määrittävät viestin formaatin ja maksutapahtuman toteuttamiseen tarvittavan menettelyn. Maksumenetelmiä ovat viestinvälitykseen liittyvät protokollat ja niitä ovat esimerkiksi **TCP/IP**, **SSL** ja **S-HTTP**.

Microsoft suosittelee SSL:n tai PCT:n käyttöä internet-tapahtumien suojaamiseen, kunnes SET-standardit ovat pidemmälle kehittyneitä. Muista joka tapauksessa aina, että menetelmä **ei** tue oikeuksien tarkistamista.

Secure Sockets Layer

Secure Sockets Layer salaa tietoyhteyksiä verkoissa käyttämällä yhdistelmää julkisen avaimen salauksesta ja tiedon salauksesta. Asiakas- ja palvelinkoneet voivat tämän protokollan avulla kommunikoida keskenään suojatusti - tällöin estetään salakuuntelua, tietojen muuttamista ja viestien väärentämistä.

SSL:n salakirjoitusavaimet luodaan samaan aikaan pareittain: julkinen avain ja yksityinen avain. Julkinen avain annetaan usein julkisen osapuolen, esimerkiksi sertifikaatin myöntäjän kautta yleiseen käyttöön. Yksityinen avain pidetään salaisena. Tiedon vaihtamiseen tarvitaan molempia avaimia. Avainpari luodaan ja luotu avain aktivoidaan **Key Managerilla**. Avain ei ole käytössä ennen kuin Key Managerin luoma sertifiointipyyntötiedosto lähetetään sertifikaatin myöntäjälle.

Internet Explorer salakirjoittaa tietoja (esimerkiksi yksityisiä tietoja sisältäviä HTML-lomakkeita) käyttämällä palvelimen **julkista avainta**. Salakirjoitettu tieto lähetetään palvelimelle, mikä purkaa salauksen **yksityistä avainta** käyttämällä. Salaus voidaan purkaa vain palvelimen hallitseman yksityisen avaimen avulla.

SSL:n käyttö

Server Sockets Layeria on tehokkainta käyttää vain yhteyksissä, jotka sisältävät yksityisiä tietoja, esimerkiksi luottokorttinumeroita, osoitteita tai yritystietoja. Koska SSL käyttää tietojen salaamiseen tietokoneen prosessoria, tietojen hakeminen ja lähettäminen SSL:ää käyttävistä hakemistoista kestää paljon kauemmin.

Internet Information Serveriä käytettäessä sijoita SSL:ää käyttävään hakemistoon vain ne sivut, jotka sisältävät tai vastaanottavat luottamuksellisia tietoja. Pidä myös SSL-hakemiston sivujen sisältö mahdollisimman yksinkertaisena, koska jokainen sivun elementti salakirjoitetaan - myös kuvat. Jokainen sivun elementti kasvattaa tietojen siirtämiseen kuluvaa aikaa.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Porotocol (PPTP) on yhteysprotokolla, joka tukee virtuaalisten yksityisverkkojen (*Virtual Private Networ*k, VPN) luomista internetistä Microsoft Windows NT Servereille. PPTP käyttää analogista tai ISDN-yhteyttä luodakseen tunnelin suoraan verkon tiettyyn NT-palvelimeen, vaikka verkossa olisi satoja NT-palvelimia. Microsoft, Ascend Communications, ECI Telematics, 3Com ja U.S. Robotics tukevat protokollaa.

Etäkäyttäjät ottavat yhteyden internetiin omasta sijaintipaikastaan. Yhteys otetaan tiettyyn PPTP-yhteyksiä hoitavaan internet-palveluntarjoajaan. Palveluntarjoaja asentaa palvelimeensa PPTP:tä tukevia **edustakoneita** (*Front-end processor*, FEP). Mikä tahansa PPP-asiakas (ei vain PPTP:tä ymmärtävä) voi luoda salakirjoitetun PPTP-yhteyden PPTP:tä tukevalle palvelimelle.

PPTP-järjestelmän käyttämiseen ei välttämättä tarvita internet-palveluntarjoajaa. Monet organisaatiot ottavat yhteyden suoraan internetiin. PPTP toimii myös näin ja tarjoaa samantasoisen tietoturvan kuin internet-palveluntarjoajan kautta käytettynäkin. Windows 95- ja Windows NT-työasemien käyttäjät voivat hyötyä menetelmästä välittömästi.

PPTP-yhteyden alustaminen Windows NT Server 4.0:lla tukee toistaiseksi vain **puhelinverkkoyhteyksien etäkäyttäjiä**. PPTP:n tulevissa versioissa Windows NT:lle tuetaan myös lähiverkkojen välisiä yhteyksiä.

Jotta internet-palveluntarjoaja voisi tarjota PPTP-yhteyksiä, sen täytyy hankkia ohjelmia tai päivittää olemassa olevan etäkäyttöpalvelimensa ohjelmisto. Kun tarvittavat päivitykset on tehty, asiakkaat voivat alkaa käyttää PPTP:n VPN-verkkoja ilman, että heidän tarvitsee muuttaa palvelimen tai tai sen asiakkaan asetuksia. Käyttäjien kirjautumisen hyväksymiseen käytetään olemassa olevia Windows NT:n etäkäyttöpalveluprotokollia, esimerkiksi **PAP**:ia, **CHAP**:ia tai **MS-CHAP**:ia. Myös internet-palveluntarjoaja voi tarvittaessa lisäksi tarkistaa oikeudet. PPTP-tiedonsiirron turvaamiseen käytetään samoja **RC4-protokollia** kuin etäkäyttöpalvelimissakin.

Microsoftin CHAP-versiota käytetään käyttäjän oikeuksien tarkistamiseen Windows NT -toimialueella. Saatavalla istuntokohtaisella avaimella voidaan salata siirrettävät tiedot. Sekä etäkäyttöpalvelin että asiakas voidaan määrittää hyväksymään vain salatut istunnot. Microsoft on ulottanut etäkäyttöpalvelimien jo olemassa olevan salaustuen myös internet-yhteyksien turvaamiseen.

Salausavainten jakelu ei ole ongelma, koska asiakaskoneella käytetään käyttäjän antamaa salasanaa ns. **hash-arvon** (hash-funktio) luomiseen. Tähän käytetään RSA MD4-salausta, ja Windows NT:n turvatietokannassa on samalla tavoin saatu arvo. Tällä menetelmällä poistetaan tiedon salaukseen ja salauksen purkamiseen tarvittavien avaimien jakeluongelma. Tiedonsalaukseen käytetään 40-bittistä istuntokohtaista avainta - joka on muodostettu aiemmin tehdyn laskutoimituksen avulla. Tulevat versiot tukevat 128-bittistä salausta.

PPTP:tä voidaan käyttää yhdessä **palomuurien** (*Firewall*) kanssa. Kun palomuuri säätelee internetistä yritysverkkoon tulevia tietoja, PPTP turvaa yhteydet hyväksyttyjen etäkäyttäjien ja yritysverkon välillä. Jos käytetään sekä palomuuria että Windows NT -etäkäyttöpalvelinta, etäkäyttöpalvelin sijoitetaan palomuurin ulkopuolelle ja se lähettää etäkäyttäjiltä tulevat paketit palomuurille. Palomuurin tehtävä on aivan sama kuin ilman etäkäyttöpalvelintakin.

File Transfer Protocol

File Transfer Protocol (FTP) on käyttökelpoinen palvelu, koska se hyväksyy tiedostoja etäkäyttäjiltä ja erilaisen tiedostojärjestelmän käyttäjiltä.

FTP käyttää aina käyttäjätason tietoturvaa, jolloin käyttäjän täytyy kirjautua järjestelmään saadakseen käyttöoikeuden FTP-palvelimelle. **Internet Information Serverin** FTP-palvelu pystyy kuitenkin käyttämään Windows NT:n käyttäjätunnistusta. Koska FTP-yhteydet välitetään salaamatta, käyttäjätunnus ja salasana jäävät kuitenkin näkyviin.

Salasanojen paljastumisen ongelma poistuu, jos FTP-palvelin konfiguroidaan hyväksymään anonyymikäyttö. Anonyymikirjautumisessa käyttäjä antaa käyttäjätunnukseksi **anonymous** ja salasanaksi internet-sähköpostiosoitteensa. NTFS:n kannalta anonyymikäyttäjät voivat käyttää tiedostoja **IUSR_koneennimi** -tunnuksella. Anonyymikirjautuminen on käytännöllinen, koska silloin oikeita salasanoja ei paljasteta julkiseen verkkoon. FTP on oletusarvoisesti konfiguroitu sallimaan anonyymikäyttö.

Internet-käyttäjille voidaan luoda **postilaatikko** tai **pudotuslaatikko** (*drop box*), johon käyttäjät voivat jättää tiedostoja. **Drop box** täytyy olla NTFS-levyllä. **Drop box** voidaan antamalla käyttäjille NTFS-tasolla vain **kirjoitusoikeus** (Write).

Kun olet määrittänyt pelkän kirjoitusoikeuden, internet-käyttäjät voivat sijoittaa **drop box** -hakemistoon tiedostoja, mutta eivät katsella tai kopioida muiden käyttäjien sinne jättämiä tiedostoja. Tiedostoja voivat lukea ainoastaan käyttäjät, joilla on riittävät oikeudet.

Domain Name System

DNS on internetin nimeämisjärjestelmä, joka sisältää jaetussa tietokannassa tiedot palvelinnimien ja IP-osoitteiden välisistä yhteyksistä. Tietokanta on olemassa useilla eri internet-palvelimilla. Monilla organisaatioilla on oma DNS-palvelimensa sisäistä käyttöä varten tai oman organisaation järjestelmän tietojen antamiseen internet-käyttäjille.

DNS sisältää myös tietoja palvelimista esimerkiksi **Mail eXchange** (MX) -tietoja, joissa määritetään toimialueelle yksi tai useampi internetistä saapuvaa postia hyväksyvä palvelin.

Sisäistä DNS-palvelua käytettäessä kannattaa muistaa, että internet-käyttäjät voivat kysellä sisäisen verkon DNS-palvelimelta tietoja sisäisen verkon tietokoneista. Tämän voi estää konfiguroimalla DNS-palvelimen siten, että ulkoiset palvelimet voivat kysellä tietoja organisaation **internet-palvelimista**, mutta **eivät** muista sisäisen verkon palvelimista. Tähän tarvitaan kaksi DNS-palvelinta. Ensimmäinen, joka vastaa ulkoisiin DNS-kyselyihin, on rekisteröity hallinta-alueeseen ja siihen on konfiguroitu esimerkiksi MX-järjestelmän tiedot ja osoite.

Tälle DNS-palvelimelle ei määritellä mitään tietoja sisäisistä järjestelmistä. Toinen DNS-palvelin vastaa sisäisiin DNS-kyselyihin ja lähettää kyselyt edelleen ulkoiselle DNS-palvelimelle, **jos** ei pysty itse vastaamaan niihin. Näin sisäisen verkon asiakkaat saavat tietoja internetin palvelimista. Ulkoisella DNS-palvelimella ei ole riittävästi tietoja sisäisistä järjestelmistä ja koska sisäiseen DNS-palvelimeen ei voida ottaa yhteyttä internetistä.

Eräs mahdollisuus hyökätä DNS-palvelimeen on pyytää siltä IP-osoitetta esimerkiksi www.satku.fi-nimisestä palvelimesta. DNS-palvelin lähettää rekursiivisen kyselyn, jolloin hyökkääjä palauttaa vastauksia, jotka väittävät IP-osoitteen www.satku.fi:lle olevan vaikkapa 127.0.0.1 tai mitä tahansa. DNS-palvelin tallentaa tämän välimuistiinsa, ja saattaa pysyä siellä kunnes DNS-palvelin resetoidaan seuraavan kerran. Tämä on ns. **Välimuistin saastutus**-hyökkäys (*Cache Pollution*), johon on olemassa korjaus kyselyiden satunnaisten tunnistetietojen muodossa osoitteessa:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/dns-fix

RPC-hyökkäys

Eräs tapa aiheuttaa ongelmia Windows NT 4.0-palvelimelle on ottaa yhteys porttiin 135 ja lähettää esimerkiksi Telnetillä komento, jota NT ei osaa tulkita. Tämä aiheuttaa CPU-kuormituksen nousun (kunnes se on 100%) ja palvelin saattaa jumiutua hetken kuluttua.

Väliaikainen ratkaisu on portin **135** kieltäminen käytöstä IP-suodatusasetuksissa.

Service Pack 3 korjaa ongelman.

Out of Band-hyökkäys

Ns. **WinNuke**-hyökkäyksen idea on lähettää NetBIOS-porttiin **139** merkkijonoja, joita käyttöjärjestelmä ei osaa tulkita - siitä tulee termi *Out of band*. Seurauksena on palveluiden (tai koko käyttöjärjestelmän kaatuminen) eli *Denial of Service*.

Service Pack 3 korjaa ongelman tuomalla lisäsuojaksia NetBIOS-porttiin **139** ja Telnet-porttiin.

Joka tapauksessa **NetBIOS over TCP/IP** tulisi estää Internetin kautta joko reitittimen tai TCP/IP:n suojausten avulla.

SYN-hyökkäys

Eräs menetelmä tukehduttaa Internet-palvelin on ns. SYN-hyökkäys (*SYN-attack* tai *SYN Flooding*).

Huomaat tälläisen olemassaolon viimeistään ilmoituksesta:

The connection has been reset by the remote host.

Hyökkäys toimii lyhyesti selitettynä seuraavasti (ks. pidempi selitys: **CERT(sm) Advisory CA-96.21** osoitteessa **ftp://info.cert.org/pub/cert_advisories**):

TCP-yhteyspyyntö (SYN) lähetetään kohteeseen, siten että lähdeosoite on muunnettu joksikin osoitteeksi, jota ei internetistä löydy. Pyyntöjä lähetetään **useita**. Kun pyynnöt tulevat, kohde varaa resursseja yhteyteen ja palauttaa vastauksen **SYN-ACK**. Koska vastauksen kohdetta ei ole, Windows NT 3.5x tai 4.0-kone (oletusasetuksin) uudelleenlähettää SYN-ACK:in 5 kertaa, tuplaten joka kerralla aikakatkaisun: 3, 6, 12, 24 ja 48 sekuntia. Lopuksi vastausta odotetaan 96 sekuntia, eli kokonaisaika on 189 sekuntia.

Jos epäilet tällaista, anna komento:

netstat -n -p tcp

Näet jotain tällaista:

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1030	127.0.0.1:1032	ESTABLISHED
TCP	127.0.0.1:1032	127.0.0.1:1030	ESTABLISHED
TCP	28.11.196.9:21	28.11.196.2:1256	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1257	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1258	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1259	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1260	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1261	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1262	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1263	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1264	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1265	SYN_RECEIVED
TCP	28.11.196.9:21	28.11.196.2:1266	SYN_RECEIVED
TCP	28.11.196.9:4801	10.57.14.221:139	TIME_WAIT

Jos suuri määrä yhteyksiä on **SYN_RECEIVED** -tilassa, syynä *voi* olla SYN-hyökkäys. Korjaus tuli jo Service Pack 1:n HotFixinä (uudemmissa se on jo mukana), katso tarvittaessa lisäohjeita:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-preSP1/syn-attack

Etäkäyttäjät

Etäkäyttäjien tietoturva on laaja aihe - tietoliikenneyhteyksien kannettavat mikrot ovat otollisia väärinkäytösten kohteita. Joitakin yleisiä ohjeita voidaan antaa:

- Anna tarkat ohjeet ihmisille, jotka matkustaessaan kuljettavat kannettavilla tietokoneilla mukanaan yrityksen tietoja tai jotka ottavat yhteyden yrityksen verkkoon etätietokoneelta käsin

- Käytä tarvittaessa ylimääräisiä tunnistusmenettelyjä etäkäyttäjille

- Käytä vaikeasti arvattavia käyttäjätunnuksia, salasanoja ja avainkorttijärjestelmiä

- Älä anna käyttäjien tallentaa salasanojaan mikron kiintolevylle. Tietokoneen varastava hakkeri voi murtaa salasanan ja kirjautua verkkoon (Työryhmä-Windowsissa voidaan estää salasanojen tallennus **ADMINCFG.EXE**-ohjelmalla ja Windows 95:ssä **POLEDIT.EXE**:llä)

- Salaa kannettavilla tietokoneilla olevat luottamukselliset tiedostot, jolloin hakkerien on vaikeaa tai mahdotonta nähdä niitä. Tähän tarkoitukseen löytyy useita ohjelmistoja

- Windows NT:n NTFS on helppo murtaa useillakin menetelmillä. Helpoin lienee **NTFSDOS.EXE**, hitain Windows NT:n asentaminen uudelleen - ilman kiintolevyn alustamista. NTFS ei siis kaikesta huolimatta tuo kannettavassa mikrossa tiedostoille mitään lisäsuojaa

- Käytä takaisinsoittojärjestelmiä, joissa tietokone soittaa etäkäyttäjälle takaisin johonkin tiettyyn ja luotettavaan puhelinnumeroon. Tämä voidaan järjestää Windows NT:n RAS-palvelimen takaisinsoittoasetuksilla

- Vaihda käyttäjätunnuksia ja salasanoja usein, samoin etäkäytön puhelinnumeroita. Jos käytät takaisinsoittoa, muuta etäpuhelinnumeroita usein, jos vain mahdollista

- GSM-datapuhelut ovat jo sinällään suojattuja GSM-verkossa, mutta kiinteän verkon yhteydet eivät ole sen enempää suojattuja kuin muutkaan puhelinverkon yhteydet.

Intranet ja internet

Internetin tietoturva on aihealue, josta löytyy huomattavasti asiantuntevia teoksia, esimerkiksi Nikander ym: **Internet tietoturva** (Suomen ATK-Kustannus Oy). Tämän luvun alussa listatuista internet-osoitteista löytyy myös runsaanlaisesti lisätietoa.

Lyhyesti sanottuna on kysymys siitä, että vaikka sisäisen verkon käyttäjät voivatkin käyttää internetiä ja toisinaan jhalutaan sallia internet-käyttäjille pääsy esimerkiksi organisaation WWW-palvelimeen, ei *yleensä* haluta, että internet-käyttäjät voivat käyttää sisäistä verkkoa täysin vapaasti.

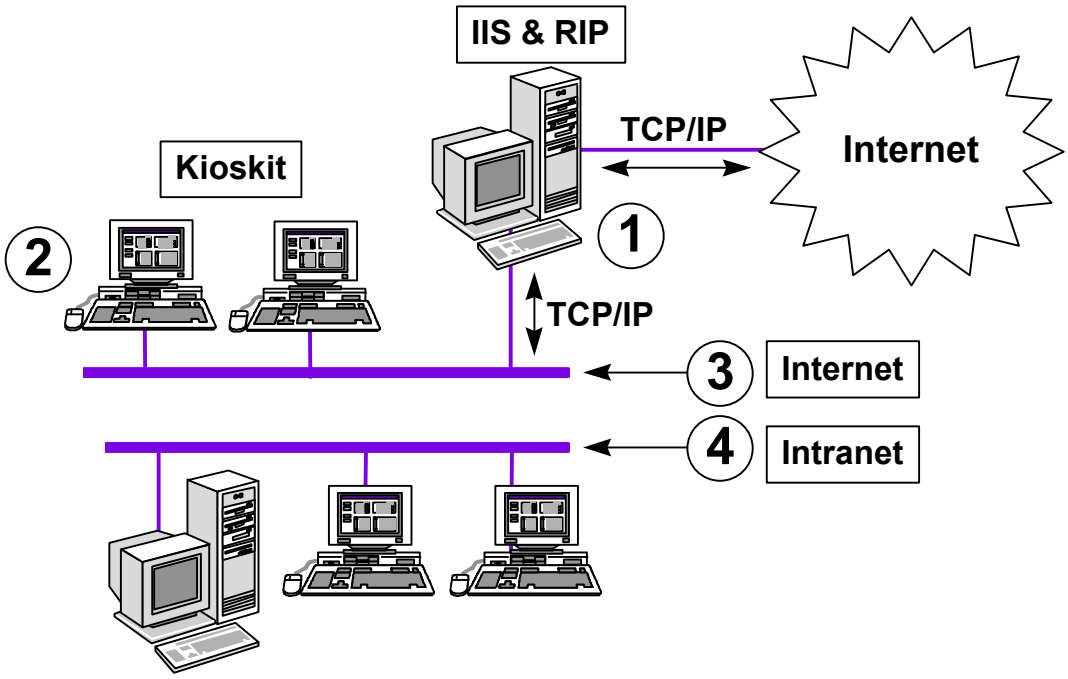
Kun **intranet** liitetään **internetiin**, sisäisessä verkossa voidaan käyttää fyysistä eristystä, protokollaeristystä, erillisiä reitittimiä ja Windows NT -reititystä turvallisuuden parantamiseen. Valittava topologia vaikuttaa intranet-käyttäjille tarjottaviin palveluihin. Seuraavassa esitellään Windows NT-ympäristössä käytettäviä menetelmiä - kirjoittaja suosittaa harkittavaksi myös ulkoisia internet-turvalaitteita ja -ohjelmistoja, vaikka niitä ei käsitellä tässä kirjassa.

Fyysinen eristäminen

Turvallisin tapa tarjota pääsy internetiin on erillinen, intranetistä irrallaan oleva Windows NT-palvelin, ja se on myös helpoin suunnitella ja konfiguroida. Palvelimeen voidaan asentaa **Internet Information Server** ja käyttää **Internet Exploreria**. Sisäistä verkkoa ei pääse selailemaan, koska siihen ei ole fyysistä yhteyttä. Itse palvelin on toki yhä altis hyökkäyksille ja se pitää konfiguroida turvalliseksi.

Tämän menetelmän haittapuoli on se, että tiedostoja ei voida jakaa intranetin ja internetin välillä. Tiedon jakamiseen järjestelmien välillä täytyy käyttää levykkeitä, Iomega Jazin tyyppisiä siirrettäviä kiintolevyjä, sarjaporttiyhteyksiä, magneettinauhoja, CD-ROMeja tai tilapäisiä verkkoyhteyksiä.

Rakennetta voidaan kehittää edelleen ja luoda pieni intranet, jonka käyttäjien työasemat ja muut IIS-palvelimet liitetään internet-palvelimeen, jossa on RIP-protokolla (*RIP for Internet Protocol Service*).



1) IIS-palvelin kahdella verkkokortilla - toinen liitetty suoraan internetiin, toinen sisäiseen internetiin liitettyyn verkkoon

2) Kioski-työasemat

3) Erillinen kaapelointi

4) Erillinen kaapelointi intranetissa

Jos organisaation käyttäjille halutaan antaa helppo pääsy internetiin, voidaan rakentaa fyysisesti täysin erillinen verkko. Verkko koostuu internet-palvelimesta, muista internet-palvelimista (kuten muista IIS-palvelimista, joihin peilataan ensimmäisen IIS-palvelimen tietoja) ja käyttäjien kioski-tyyppisistä työasemista. Kioskit voivat sijaita kokoushuoneissa, auloissa, kirjastoissa tai erityisissä toimistoissa koko yrityksessä. Internetiä paljon käyttävillä työntekijöillä voi olla omat kioski-työasemansa. Kioskien kautta voidaan hakea tietoa internet-palvelimelta, sijoittaa palvelimelle uutta tietoa ja kerätä tietoja internetistä. Tällaisessa mallissa tarvitaan kuitenkin lisäkaapelointia. Lisäksi kaapelointien pitäminen erillään saattaa olla haasteellinen tehtävä.

Muuta tarkistettavaa:

- Sallitut portit IIS-palvelimessa (ks. Luku 9)
- SMB-palvelut IIS-palvelimessa
- IIS:n kirjausmenettelyt.

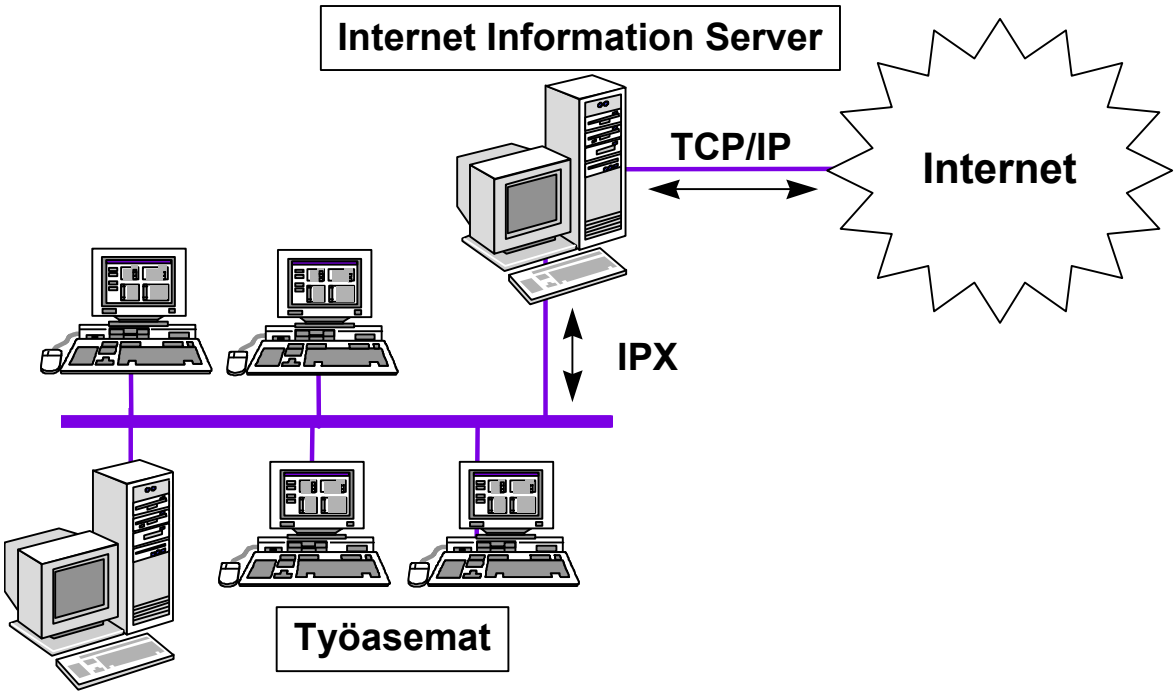
Erilliset protokollat

Jos sekä internet- että intranet-tietokoneiden halutaan olevan yhteydessä Internet Information Server-palvelimeen turvallisuus voidaan taata käyttämällä eri protokollia. Tässä mallissa internet-palvelimessa on kaksi verkkokorttia, joista Internetiin kytketty verkkokortti käyttää TCP/IP-protokollaa ja intranetiin liitetty sovitin mitä tahansa protokollaa (esimerkiksi IPX) paitsi TCP/IP:tä.

Intranet-käyttäjät voivat kopioida tiedostoja ja ylläpitää palvelinta. He eivät kuitenkaan pääse IIS-palvelimelle, koska sinne pääsemiseen tarvitaan TCP/IP-protokollaa. Internet-käyttäjät pääsevät IIS-palvelimeen, mutta eivät pääse intranetiin, koska siihen vaaditaan esimerkiksi IPX-protokollaa.

Eri protokollien käyttöön perustuva turvajärjestely sopii parhaiten käyttäjille, jotka käyttävät suurimman osan ajastaan tietojen tuottamiseen internet-käyttäjien saataville ja jotka haluavat kopioida tiedostoja suoraan intranetistä internet-palvelimelle. Se sopii myös käyttäjille, jotka noutavat usein internet-käyttäjien **pudotuslaatikkoon** (*drop box*) jättämiä tiedostoja.

IIS-palvelimen resursseja voidaan käyttää molemmista suunnista, mutta tietoja ei voida välittää sen kautta.



Menetelmän etuna on se, että käyttäjät voivat jakaa tietoa internet-käyttäjien kanssa omalta intranet-työasemaltaan käsin ilman riskiä, että intranet joutuisi luvattoman käytön kohteeksi.

Ratkaisun huonoja puolia:

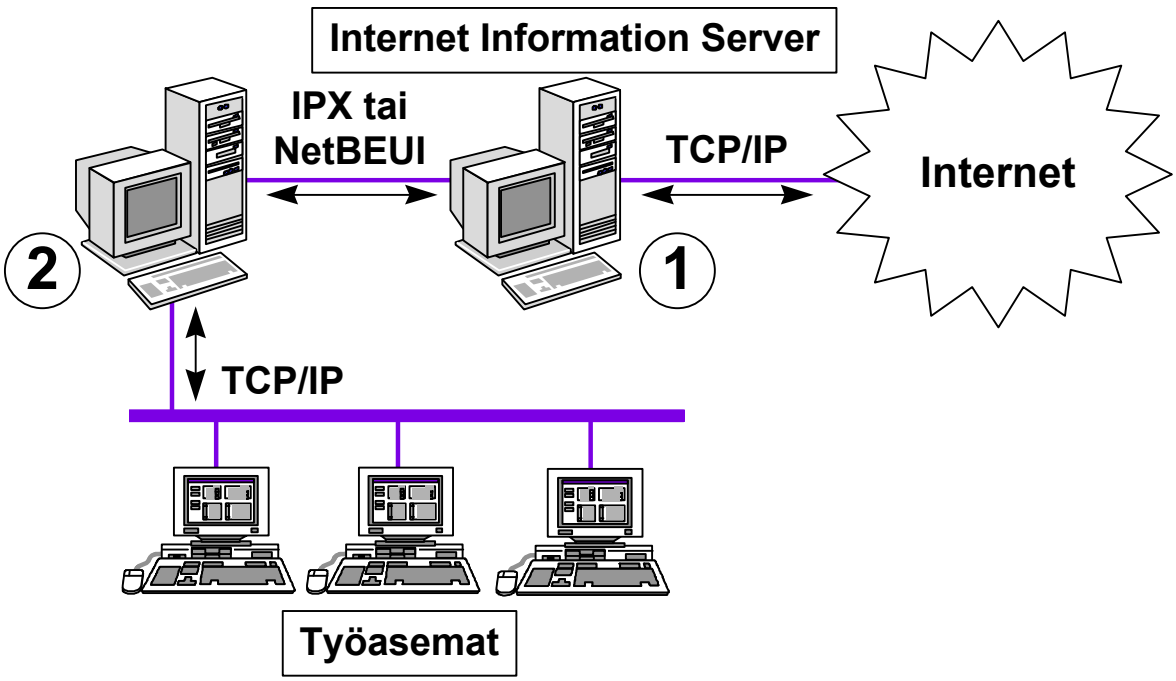
- Käyttäjät eivät pääse suoraan internetiin tai IIS-palvelimelle
- Käyttäjät eivät voi etsiä tai hakea internet-resursseja, vaan ainoastaan Windows NT -palvelimella olevia resursseja
- Käyttäjät eivät myöskään voi lähettää sähköpostia muiden internet-käyttäjien kanssa (ellei palvelimelle ole asennettu internet-postipalvelinpalvelua).

Internet-käyttäjä voi ainakin teoriassa kuitenkin tunkeutua sisäiseen verkkoon. Se on kuitenkin erittäin vaikeaa, koska palvelimella ei tehdä protokollamuunnoksia.

Internet-palvelimen peilaus

Variaatio eri protokollien käytöstä on monistaa internet-palvelimella olevat tiedot Windows NT:n monistus (*Replication*) -palvelun avulla toiselle sisäisen verkon palvelimelle. Apuna voidaan käyttää myös ajastettuja komentojonoja ja/tai Resource Kitin **ROBOCOPY**-ohjelmaa.

Jos internet-palvelinta käytetään pudotuslaatikkona, johon asiakkaat voivat jättää viestejä ja ehdotuksia, tiedot kopioidaan automaattisesti internet-palvelimesta intranet-tietokoneelle. Tiedonsiirto voi olla myös kahdensuuntaista. Koska palvelimet ovat eristettyjä toisistaan protokollatasolla, intranetin NT-palvelimessa voidaan myös ajaa Internet Information Serveriä internet-sivujen sisäisenä versiona. Tätä mallia käytetään mm. Microsoftin yritysverkossa.



1) IIS-palvelin kahdella verkkokortilla - toinen liitetty suoraan internetiin, toinen sisäisen intranetin IIS-palvelimeen

2) IIS-palvelin kahdella verkkokortilla - toinen liitetty suoraan intranetiin, toinen internetiin liitettyyn IIS-palvelimeen

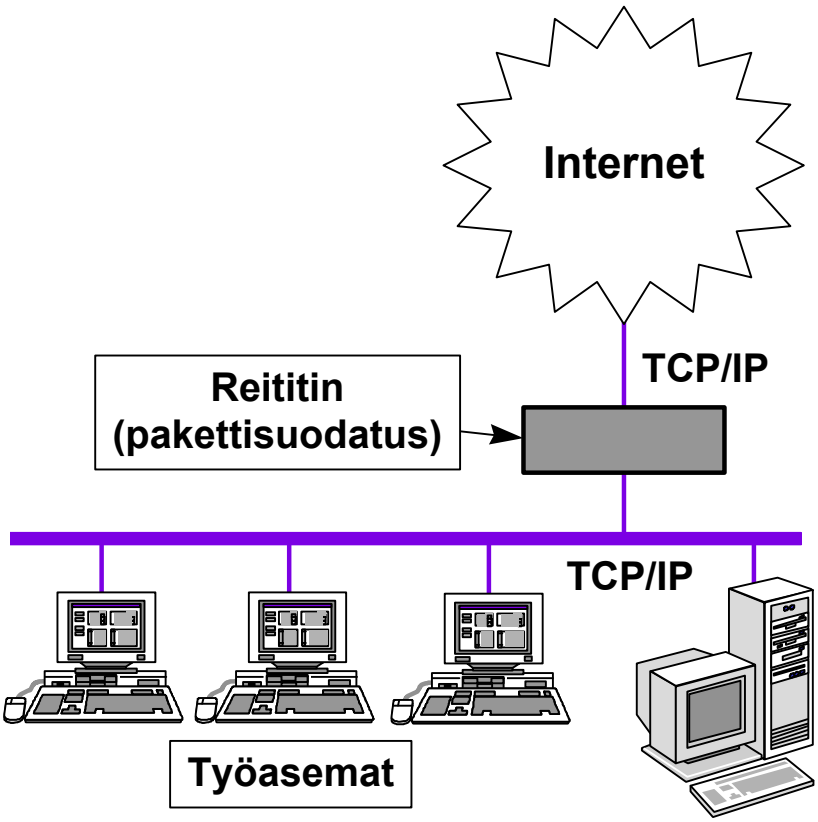
Tässä peilausmallissa voidaan myös paremmin valvoa, mitä tietoja tuodaan intranetiin ja mitä lähtee ulos: tiedostoista voidaan mm. etsiä viruksia. Intranetissa voidaan käyttää TCP/IP-protokollaa, koska intranetin ja internetin välinen IPX- tai NetBEUI-osuus eristää protokollat toisistaan.

Erillinen reititin

Jos TCP/IP:tä käytetään laajoissa intraneteissä, joissa on monia aliverkkoja, kannattaa käyttää erillistä reititintä ja yhteyttä internetiin. Reitittimet voidaan konfiguroida **suodattamaan paketteja** niiden lähde- tai kohde-IP-osoitteen perusteella. Niihin voidaan määrittää, mistä IP-osoitteista sallitaan tai kielletään pääsy sisäiseen verkkoon. Lisäksi voidaan määritellä sallitut portit, joiden kautta päästään tietokoneessa käynnissä olevaan ohjelmaprosessiin - esimerkiksi HTTP-palvelimet toimivat portissa **80**.

Suodatusta käyttämällä voidaan estää sisääntuleva liikenne epäluotettaviksi tiedetyistä tai ei-toivotuista verkoista. Pakettien suodatus ei kuitenkaan ole luotettava tietoturvakeino, koska murtautuja voi yksinkertaisesti käyttää tietokonetta, jolla on eri IP-osoite. Toisaalta suodatuksella voidaan estää ei-toivotuista lähteistä tulevat liikennöintitulvat.

Suodatuksen avulla voidaan myös estää tiettyjä sisäisiä käyttäjiä pääsemästä WWW-palvelimellesi. Tämä voidaan tehdä liikennöintiongelmien pienentämiseksi tai estämään tarpeeton pääsy palvelimelle.



Voidaan myös estää FTP:n ja TELNETin kaltaisten palveluiden käyttö. Tunkeilijat käyttävät TELNETin kaltaisia ohjelmia yrittäessään murtautua järjestelmään. Toisaalta voidaan estää kaikki liikenne koko palvelimeen lukuunottamatta jotakin tiettyä porttia.

Esimerkiksi sähköpostiyhdyskäytävä voidaan asettaa porttiin **25**, joka on **SMTP** (*Simple Mail Transfer Protocol*) -palvelu. Jos pidät yllä DNS:ää (*Domain Name Service*, DNS-nimipalvelin), tunkeilijat voivat yrittää päästä käsiksi sen tietokantaan, etsiä sisäisen verkon palvelimien tiedot ja sitten yrittää naamioitua joksikin sisäisen verkon järjestelmäksi.

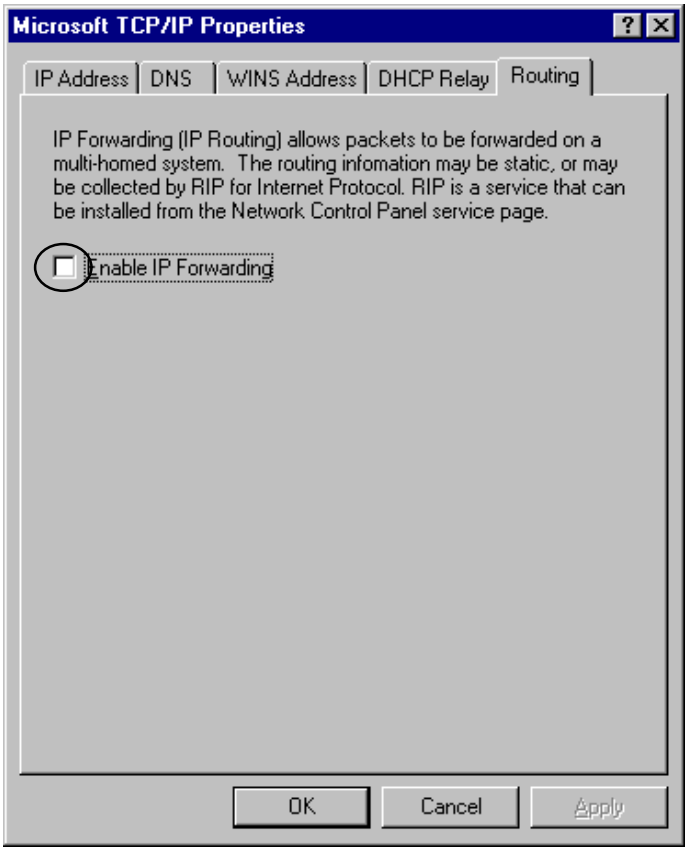
Palvelu	**Portti**
TELNET (pääte-emulointi)	23
FTP (File Transfer Protocol)	20 ja 21
SMTP (Simple Mail Transfer Protocol)	25
RIP (Routing Information Protocol)	520
DNS (Domain Name System)	53
HTTP (HyperText Transfer Protocol)	80

Tässäkin asiassa voi turvautua niin moneen puolustusstrategiaan kuin mahdollista. Vaikka suodatus onkin joissakin tapauksissa tehokas menetelmä, se ei ole suinkaan mikään kokonaisratkaisu. Suodattamalla voidaan ehkä torjua jollakin tietyllä IP-osoitteella murtautumista yrittävän tunkeilijan, mutta hän saattaa onnistua käyttämällä jotakin toista IP-osoitetta.

Microsoft **Internet Information Server**issä on mahdollista toteuttaa pakettien suodatus sallimalla tai kieltämällä pääsy joihinkin tiettyihin IP-osoitteisiin. Lisäksi poikkeukset voidaan sallia.

Windows NT -reititys

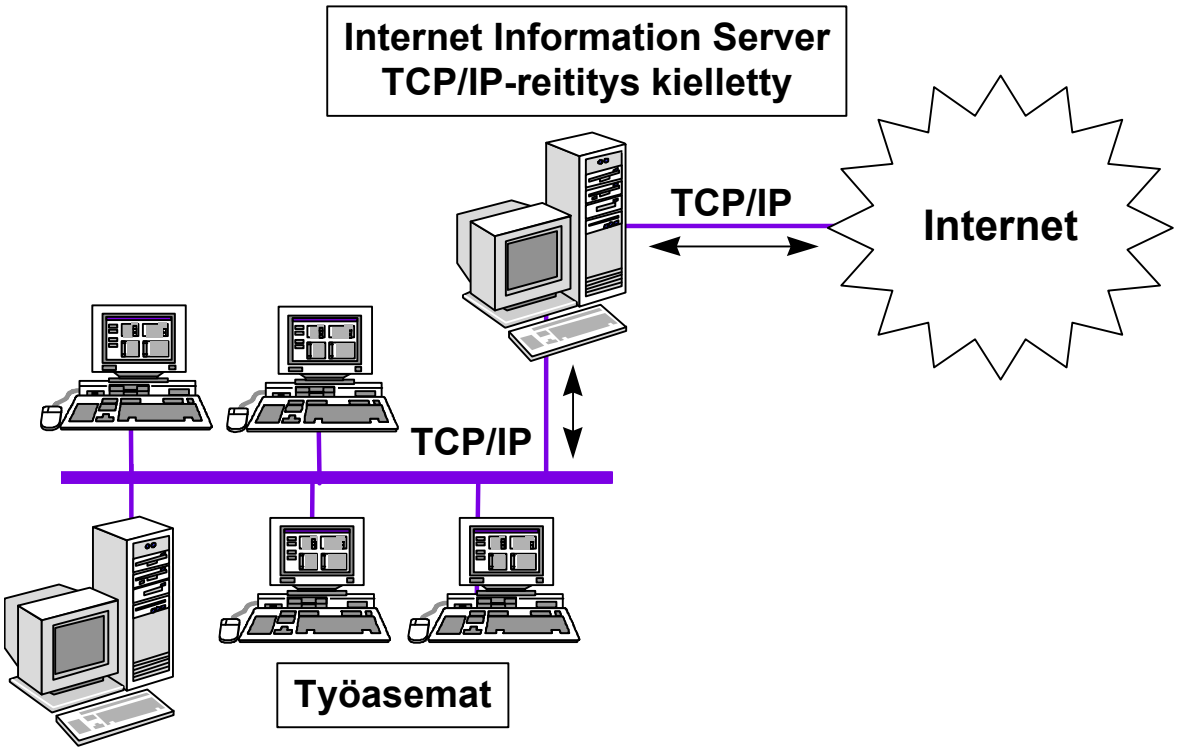
Jos intranetissä käytetään TCP/IP-protokollaa, Windows NT -palvelimesta voidaan luoda eräänlainen palomuuri estämällä TCP/IP-reititys. Internet Information Serverin palvelut ovat silti saatavilla yhä sekä intranet- että internet-käyttäjille.



TCP/IP-reititys valvoo, sallitaanko pakettien liikenne Windows NT

-palvelimen kautta eli se valvoo, toimiiko palvelin yhdyskäytävänä. Reititinominaisuus toimii vieläpä molempiin suuntiin - liikenne kulkee palvelimen kautta joko molempiin suuntiin tai se ei kulje lainkaan.

Tällä mallilla on kaikki erillisten protokollien mallin edut ja haitat: suuri ongelma tässä mallissa on se, että internetin ja intranetin erillisyys riippuu yhdestä ainoasta TCP/IP-konfiguraation (tai rekisterin) asetuksesta. Windows NT -palvelimessa tarvitsee muuttaa (vaikkapa vain vahingossa) yhtä ainoaa asetusta, ja sisäiseen verkkoon on täysi pääsy internetistä (ks. myös luku 9).



Jos käytetään tätä turvallisuusmallia, täytyy kiinnittää erityistä huomiota Internet Information Server-palvelimen fyysiseen turvallisuuteen ja pääkäyttäjien oikeuksiin. Windows NT:n pääkäyttäjän konfigurointityökalut ja oikeudet tunteva henkilö voi muuttaa asetusta muutamassa minuutissa - *myös* verkon kautta!

Muista seuraavat valvontamahdollisuudet:

- Käyttäjätunnusmenetelmien konfiguroiminen IIS:n käytön valvontaan **IUSR_koneennimi** -käyttäjätunnuksen avulla

- Tiedostojärjestelmien käyttö pääsyn estämiseksi tietyille levyn osille ja valvontatiedoston käyttö

- Event Viewerin turvalokin käyttö Internet Information Serveriä ajavan koneen käytön ja kaikkien Internet Information Serverin kautta käytettävien NFTS-tiedostojen valvontaan

- Internet Information Server -lokien käyttö IIS-palvelujen käytön seuraamiseen.

Vapaa pääsy internetiin

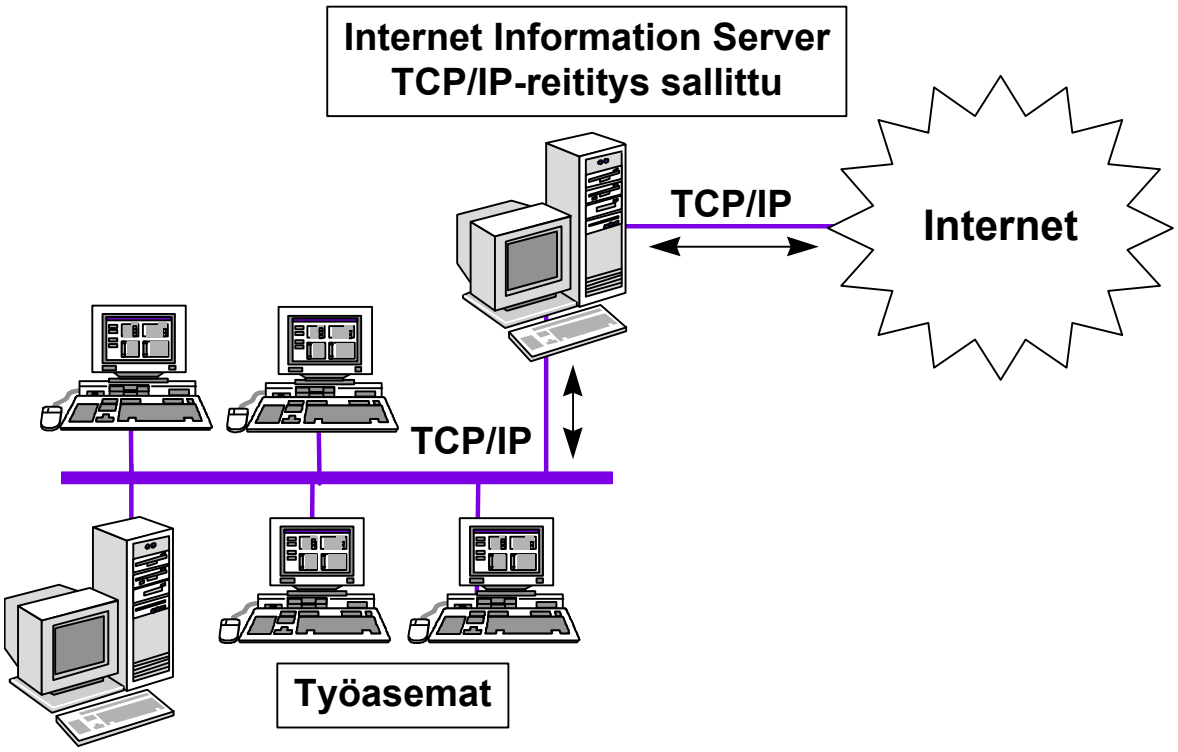
Joissakin organisaatioissa tarvitaan käyttäjille vapaa internet-yhdyskäytävä sekä internetiin että internetistä intranetiin. Yksi Windows NT -palvelin voi toimia yksinkertaisena yhdyskäytävänä internetiin. Yhdyskäytävänä toimivalla tietokoneella täytyy olla:

- Internet-yhteys

- TCP/IP-protokolla

- RIP for Internet Protocol-palvelu.

Internet Information Serveriä voidaan haluttaessa ajaa yhdyskäytävätietokoneella.



Huomaa, että reititys toimii molempiin suuntiin! Windows NT:n reitityksen huono puoli on se, että liikenne pääsee kulkemaan palvelimen kautta molempiin suuntiin tai se ei pääse lainkaan. Jos mahdollistetaan **RIP for Internet Protocol** intranetin luottamukselliset tiedot täytyy suojata muilla tavoin esimerkiksi NTFS-suojausten avulla.

Eri asia sitten on, onko sekään riittävää, koska Windows NT:tä, Työryhmä-Windowsia, LAN Manageria tai MS-DOS -työasemasta pääsee internetin kautta mihin tahansa verkon tietokoneella olevaan resurssiin käyttämällä **NET USE**-komentoja (selaus ei todennäköisesti toimi). Vain Windows NT:n turvaominaisuudet antavat suojaa tällaista käyttöä vastaan.

Palomuurit

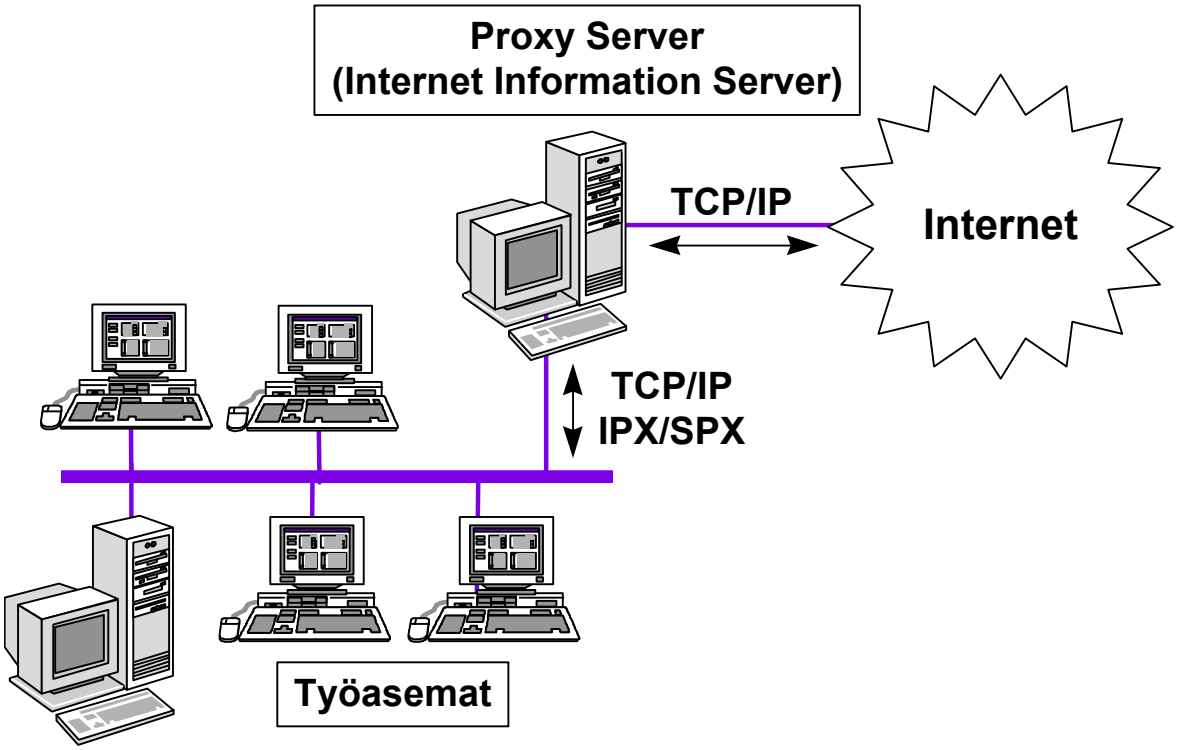
Verkon turvaamiseen ja käytön valvontaan voidaan käyttää muitakin menetelmiä kuin verkkotopologian eri vaihtoehtoja, esimerkiksi palomuureja.

Toinen suojausmenetelmä on Internetin ja intranetin väliin asennettavat erilliset **palomuurit** (*Firewall*). Useimmat tällaiset tuotteet perustuvat pakettien suodatukseen. Suodatus tapahtuu, kun tietokone tutkii paketin

lähde- ja kohde-IP-osoitteen ja lähettää sen eteenpäin vain, jos paketille on myönnetty pääsy. Myös Windows NT:lle on saatavissa palomuurituotteita, esimerkiksi Microsoft Proxy Server.

Microsoft Proxy Server (*Catapult*, ks. Luku **9**)-palvelin toimii palomuurina internetin ja sisäisen verkon välillä toimien sekä tietoa varastoivana että sitä edelleenlähettävänä järjestelmänä. Sen palomuuriominaisuudet sisältävät asetuksia, joilla se voidaan konfiguroida estämään ja suodattamaan verkkoliikennettä. Se mm. toimii siis sisäisen ja ulkoisen verkon välillä protokollakääntäjänä ja valvoo käyttöoikeuksia.

Proxy Serverin palomuuritoiminto edellyttää Windows NT-palvelinta, jossa on vähintään kaksi verkkokorttia, yksi sisäiselle verkolle ja toinen internet-liittymää varten. Kaikkien pyyntöjen ja vastausten on kuljettava Proxy Serverin kautta. Proxy-palvelin vastaanottaa sisäisiltä ja ulkoisilta käyttäjiltä tulevat FTP-, HTTP-, TELNET-, Gopher- ja WAIS-pyynnöt, tutkii ne ja lähettää ne edelleen kohdepalvelimille, jotka vastaavat pyyntöihin.



Proxy-palvelin on tehokas vain siinä tapauksessa, että internetin ja sisäisen verkon välillä ei ole **muita** suoria yhteyksiä. Käyttämällä salakirjoitusta tukevia protokollia, kuten SSL:ää (*Secure Sockets Layer*) ja PCT:tä (*Private Communication Technology*) saadaan turvalliset yh-

teydet internetin kautta.

Proxy Server-palvelimen lisäominaisuutena se tallentaa usein haettuja tietoja paikallisessa välimuistissa (*Cache*) siltä varalta, että samaa tietoja haetaan myöhemmin. Sisäisen verkon käyttäjien kannalta tämä on vain eduksi, koska välimuistissa saattaa olla valmiina esimerkiksi pyydetty internetin WWW-sivu. Menetelmä sisältää kuitenkin joitakin tietojen ajantasaisuuteen liittyviä ongelmia.

Internet-palvelimen suojaaminen

Kun käytät Windows NT:tä Internet-palvelimena, voit noudattaa seuraavia menetelmiä palvelimen suojaamisessa:

- Käytä NTFS:ää, älä FAT-tiedostojärjestelmää. Voit käyttää tarvittaessa CONVERT-komentoa muuntamaan FAT NTFS:ksi
- Jaa mahdollisimman vähän hakemistoja (jos ollenkaan) Internet Information Server-palvelimesta
- Uudelleennimeä Administrator-käyttäjätunnus
- Ota pois käytöstä Guest-käyttäjätunnus (*disabled*)
- Käytä valvontaominaisuuksia (*Auditing*) varsinkin epäonnistuneiden toimintojen (*Failures*) seurantaan. Muita kohteita ovat **Security Policy Changes** ja **Restart**. Suojaa lokitiedostot ja tallenna ne säännöllisesti
- Ota pois käytöstä **NetBIOS over TCP/IP** poistamalla sidokset (*Bindings*). Jätä TCP/IP käyttöön ja voit myös jättää sidokset NetBEUI-protokollalle, koska se ei ole reitittävä protokolla
- Sulje käytöstä tarpeettomat TCP/IP-portit - esimerkiksi FTP- ja WWW-palvelin tarvitsee sisääntuleviksi porteiksi vain **21** ja **80**. Voit sallia vain nämä portit reitittimessä tai NT:n TCP/IP-asetuksissa. **NetBIOS over TCP/IP** käyttää portteja **UDP 137**, **UDP 138** ja **TCP 139**. Näiden käytön voi estää vastaavasti
- Voit estää verkkokäytön **Access from Network** -asetuksella. Poista oikeus ainakin **Everyone**-ryhmältä - voit samalla poistaa

oikeuden muiltakin käyttäjiltä ja käyttäjäryhmiltä. Syy tähän on se, että IIS:n WWW- ja FTP-palvelimet tyypillisesti käyttävät paikallista käyttäjätunnusta. Muut FTP-palvelimet sen sijaan saattavat edellyttää kirjautumista verkon kautta tai ne käyttävät järjestelmän paikallista SYSTEM-käyttäjätunnusta

- Älä jaa tarpeetonta tietoa järjestelmästäsi ulkopuolisille (NT-versio, Service Pack-versiot, IP-osoitteet, resurssit jne)

- Älä aja tarpeettomia palveluita IIS-palvelimessa

- Poista tiedostokytkennät **.BAT**- ja **.CMD**-tiedostoilta äläkä käytä niitä CGI-scripteinä (**http://www.omna.com**)

- Poista tarpeettomat ohjelmatiedostot ja valvontatyökalut palvelimen kiintolevyltä

- Luo erilliset levyosiot järjestelmää, FTP-, HTML- ja mallitiedostoja sekä CGI-scriptejä varten

- Käytä proxy-palvelinta

- Käytä sopivia työkaluja järjestelmän heikkouksien kartoittamiseen, esimerkiksi portti- ja palveluskannereita (**http://www.iss.net**).

Kioski-työaseman suojaaminen

Joissakin tilanteissa - vaikkapa kioski-tyyppisessä työasemassa - voi olla eduksi rakentaa vain rajoitettuun käyttöön (esimerkiksi vain Internet Explorer 3.0) soveltuva Windows NT-työasema (ks. myös luvut **4** ja **5**). Ole varovainen!

Se tehdään seuraavasti:

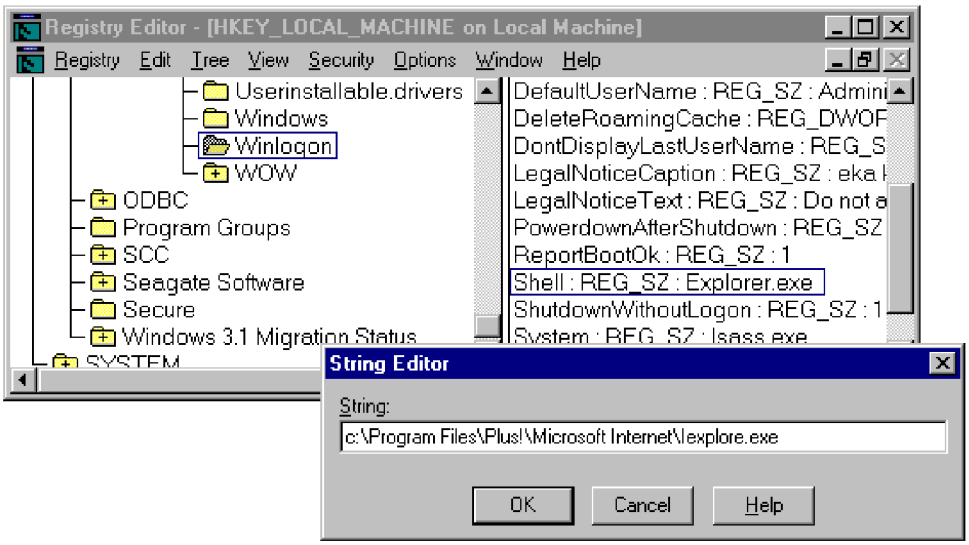
1) Alusta tai konvertoi työaseman levyt NTFS-tiedostojärjestelmällä

2) Ota käyttöön NT-työasemassa (ei toimialueella) Guest-tunnus - sillä on jo oletuksena minimioikeudet järjestelmässä. Ota työasema mukaan toimialueelle

3) Älä salli salasanan muuttamista eikä järjestelmän sammuttamista (työaseman **User Managerissa**: **Policies** | **User Rights**).

4) Korvaa käyttöliittymä: **Explorer.exe** vaihdetaan **Internet Exploreriin**:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\Windows NT\CurrentVersion\Winlogon**
Nimi	**Shell**
Tyyppi	**REG_SZ**
Arvo	Anna polku EXE-tiedostoon, esimerkiksi **C:\Program Files\Plus!\Microsoft Internet\Iexplore.exe**



5) Muuta oikeudet **%Systemroot%\System32\Taskmgr.exe** -tiedostoon siten, että Guest-käyttäjän oikeus on **No Access**. Tällöin ei pääse kirjautumisikkunassakaan Task Manageriin.

6) Uudelleennimeä paikallinen **Administrator**-käyttäjätunnus (vaikkapa **kfm034dae**) ja anna sille mukava salasana (vaikkapa **9dfkKKmfhOo0**)

7) Aseta rekisteriin **AutoAdminLogon** - vain **tehokäyttäjät** tietävät,

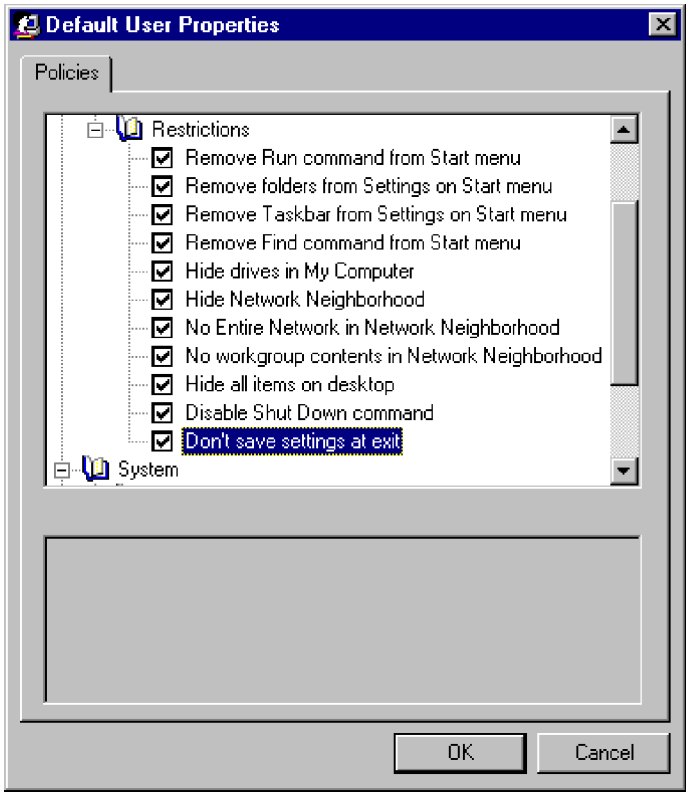
että sen voi ohittaa **vaihtonäppäimellä**

8) Ota pois käytöstä **ShutdownWithoutLogon** - se on samassa rekisterin avaimen alla kuin edellinen **Shell**-arvo - anna **0**

9) Luo oletusjärjestelmäkäytäntö (Default System Policy) joka sallii vain **Iexplore.exe**:n ajamisen ja tallenna se joko **NETLOGON**-jakoon **tai** määrittele manuaalinen päivitys ja tallenna se työaseman NTFS-levylle suojattuun hakemistoon (**Default User** | **Properties** | **System** | **Restrictions** | **Run only allowed Windows applications**). Voit myös määritellä muita sovelluksia. Jos kiellät **POLEDIT.EXE**:n käytön, muista jättää itsellesi takaportti!

10) Määrittele rajoitukset **Shell** | **Restrictions** -kohdassa niin, että käyttäjä näkee vain **%Systemroot%\Profiles\Guest\Desktop**-hakemiston

11) Voit myös rajoittaa käyttöliittymää poistamalla **kaiken Shell** | **Restrictions**-asetuksilla



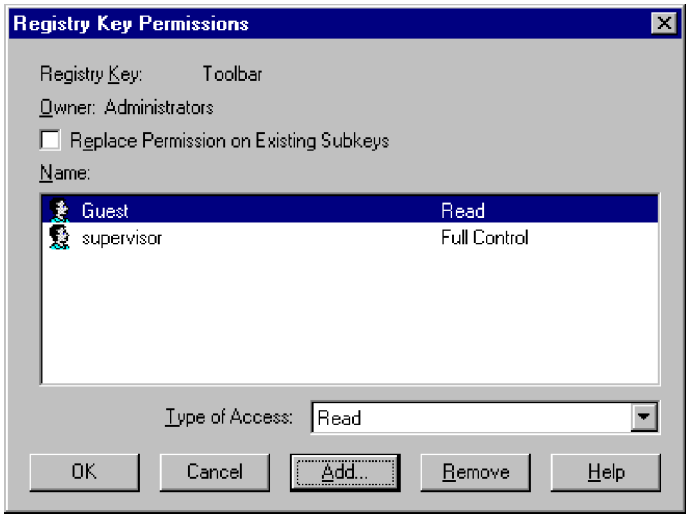
12) Internet Explorer 3.0:ssa voit poistaa osoiterivin ja muutakin

tarpeen mukaan valitsemalla **Näytä** | **Asetukset** | **Yleiset** (View | Options | General)

13) Avaa rekisterieditorissa:

Polku	**HKEY_CURRENT_USER\SOFTWARE**
Avain	**\Microsoft\Internet Explorer**
Nimi	**Toolbar**
Oikeus	**Guest-käyttäjälle vain lukuoikeus (read)** (muut ennalleen)

ja valitsemalla **Security** | **Permissions** anna Guest-käyttäjälle lukuoikeudet Toolbarin asetuksiin.



14) Kun käyttäjä kirjautuu, Internet Explorerin asetukset voivat olla väärin, mutta ei niitä ainakaan voi muuttaa!

Voit vielä kehittää lisäsuojauksia edellisten esimerkkien avulla - esimerkiksi poistaa järjestelmänhallinnan tiedostoja kiintolevyltä, suojata BOOT.INI jne - fyysisestä turvallisuudesta puhumattakaan!

Sähköposti

Sähköpostin suojaamisessa voi noudattaa seuraavia menetelmiä:

- Laadi tarkat ohjeet, joissa määritetään sähköpostin asianmukainen käyttö
- Pidätä itsellesi oikeus valvoa sähköpostin käyttöä (esimerkiksi sanomamäärät ja sanomien koko)
- Tee turvatarkastuksia ja suojaudu viruksia vastaan
- Harkitse, olisiko syytä käyttää salausta tai sähköisiä nimikirjoituksia
- Varmistu postipalvelimen fyysisestä turvallisuudesta
- Huolehdi, että käyttäjät ovat tietoisia turvavaatimuksista
- Kehitä menettelytavat arkistojen tuhoamista ja/tai säilyttämistä varten
- Pyydä käyttäjiä hyväksymään (allekirjoituksellaan) sähköpostin käyttösäännöt.

Windows NT-ympäristössä **Exchange Server** voi vähentää sähköpostin turvallisuusriskejä. Windows NT suojelee järjestelmää kaikilla turvaominaisuuksillaan, joihin kuuluvat mm. käyttäjätunnusten keskitetty hallinta, käyttöoikeudet ja valvonta. **Windows NT Challenge/Response** -turvajärjestelmä tunnistaa käyttäjät, eikä salasanoja koskaan lähetetä salaamattomassa muodossa.

Kaikki yhteydet asiakkaan ja palvelimen välillä käyttävät **Remote Procedure Call** (RPC) -protokollaa, jossa on tunnistustoiminto ja sekä salakirjoitus myös internetin kautta viestittäessä. Windows NT:n RPC käyttää RSA Data Securityn RC4-algoritmia 40-bittisellä avaimella.

Virustorjunta

Virustorjuntaa on syytä harjoittaa myös Windows NT-ympäristössä. Seuraavassa eräiden virustyyppien aiheuttamia ongelmia Windows NT:ssä:

Käynnistyslohko- tai MBR-virukset:

- Kun ja jos Windows NT on käynnistyy, ne eivät toimi
- Eivät voi tarttua edelleen NT:n käynnistyttyä
- Windows NT *ei* käynnisty, jos Master Boot Record (MBR) muuttunut tai siirretty muualle levyllä. Ratkaisuna on palauttaa MBR esimerkiksi korjauslevykkeeltä.

DOS- ja Windows 3.1-virukset **ntvdm**:ssä:

- Jos komentotulkki **CMD.EXE** tai **COMMAND.COM** on saastunut, jokainen DOS-sessiossa käynnistetty ohjelma saattaa saada tartunnan!
- Ratkaisuna on DOS-tilan skannaus. Voit myös määritellä näihin tiedosttoihin vain lukuoikeudet

Windows NT-virukset:

- Kova koodaaminen. Näitä ei juuri tunneta, koska *toistaiseksi* Windows NT-ohjelmoijille on riittänyt muutakin puuhaa.

Makrovirukset:

- Tuhoisin ja tunnetuin Winword.concept. Toimivat toki myös Windows NT:ssä ajettavissa sovelluksissa.

Ennaltaehkäisy on paras puolustus. Joitakin suosituksia:

- Ei multibuuttia varsinkaan Windows NT Serveriin
- Käytä NTFS:ää
- Käytä torjuntaohjelmaa: Norton AntiVirus for WinNT, McAfee NetShield, Dr Solomon AntiVirus Toolkit for NT

Lisätietoja:

- http://www.ncsa.com
- http://www.csi.com
- http://www.symantec.com
- http://www.mcafee.com

Virustuneet tiedostot poistetaan etsintäohjelmalla:

- Tarkista myös varmuuskopiot ja kaikki mahdolliset levykkeet
- Tiedota löytyneestä viruksesta asiallisesti

FAT-levyt:

- Käynnistys puhtaalta käyttöjärjes-telmälevykkeeltä (kirjoitussuojaus)
- Varmistuskopio kiintolevystä (datatiedostot)
- Tarvittaessa matalan tason alustus (low-level format), uudelleenosiointi ja alustus (Fdisk ja Format)
- Fdisk /MBR uudelleenkirjoittaa käynnistyslohkon (MS-DOS 5.0/6.x)

NTFS/HPFS-levyt:

- Ongelma on ehkä saada Windows NT henkiin. Voit siirtää kiintolevyn toiseen Windows NT-koneeseen, ja sitten käyttää poisto-ohjelmaa

Levykkeet:

- Poisto-ohjelma
- Sys a: uudelleenkirjoittaa käynnistyslohkon

Tee itsellesi tohtorointilevyke (FAT-levyille):

- MS-DOS 7.0-käynnistyslevyke
- Etsintäohjelmia
- Muista kirjoitussuojaus!

Menetelmäohjeita:

- Valvo ohjelmien jakamista viruksien leviämisen estämiseksi
- Valvo julkisten ohjelmien (esimerkiksi sharewaren ja ilmaisohjelmien) käyttöä
- Aja koko järjestelmässä säännöllisesti virustenetsintäohjelmia ja käytä niistä aina viimeisimpiä versioita
- Tarkista tuntemattomasta lähteestä tulleet tiedostot aina virustenetsintäohjelmalla
- Kouluta käyttäjiä suhtautumaan asiallisesti virusongelmaan
- Lukitse yleisissä tiloissa tietokoneet, jotta niihin ei voida kopioida viruksia suoraan (tai sulje levykeasemat käytöstä)
- Pysyttele ajantasalla viruksista.

Tiedostojen kopiointi Internetistä

Eräs huolenaihe on Internetistä kopioitavt (*imuroitavat*) apuohjelmat, laajennukset, testiohjelmat jne. Tämän hallitsemiseen ja estämiseen on Microsoft-ympäristössä ainakin kaksi menetelmää:

- **Microsoft Internet Explorer Administrator s Kit** (IEAK), jolla voidaan määritellä haettavien tiedostojen tyypit. Muita asetuksia ovat esimerkiksi **Allow downloading of active content**, **Enable ActiveX controls and plug-ins**, **Run ActiveX scripts** ja **Enable Java programs**
- **Microsoft Proxy Serveriä** voi laajentaa **InterScan WeProtect**- ja **Trend Micro Inc**:in tuotteilla, jolloin voidaan estää hallitsematon ActiveX- ja Java-appletien kopiointi. Periaatteena on esimerkiksi sallia vain **Authenticode**lla hyväksyttyjen (*Signed*) tiedostojen kopiointi.

Lisätietoja:

http://www.antivirus.com/webprotect.html
http://www.antivirus.com/alert/pmicros.html

12. JÄRJESTELMÄN KÄYTTÖÖN-OTTO JA YLLÄPITO

Tässä luvussa käsitellään Windows NT-järjestelmän käyttöönottoa ja ylläpitoa esimerkkien ja vinkkien avulla.

Käyttöönotto

Verkon pystytys sinänsä on helpoin vaihe Windows NT-järjestelmän käyttöönotossa. Varsinainen työ alkaa, kun ensimmäinen käyttäjä kirjoittautuu toimialueelle ja ensimmäiset resurssit saadaan käyttöön verkosta.

Usein jotain on jo pielessä tässä vaiheessa.

Käyttäjätunnuksista, varmistuksista ja oheislaitteista huolehtiminen ei suinkaan ole ohi asennuksen jälkeen - myös ylläpitoon pitää varata omat resurssinsa. Tyypillisesti odotetaan, että *joku* ylläpitää verkkoa oman toimensa ohessa. Vastuualueet *on* syytä täsmentää ajoissa.

Kuten minkä tahansa ATK-järjestelmän, myös Windows-verkon pystytys voidaan ytimekkäästi tiivistää kolmeen sanaan: **suunnittelu, testaus sekä standardointi**. Testaukseen voidaan katsoa kuuluvan myös opiskelu.

Muista suunnittelussa paitsi käyttäjälähtöinen-, myös tekninen lähestymistapa. Tämä tarkoittaa sitä, että hyvä verkko on erinomainen paitsi käyttäjän, myös tuen kannalta.

Suunnittelu

Suunnittelu voidaan aloittaa **nykytilanteen** tarkastelusta:

- Mitä on tällä hetkellä olemassa (laitteet, ohjelmat, verkon osat) ja miten niitä käytetään

- Mitkä ulkopuoliset yhteydet halutaan (Internet, puhelinverkkoyhteydet, ISDN...)
- Mistä olemassaolevasta järjestelmästä tai sen osasta ei haluta luopua ja miten se integroidaan Windows -verkkoon (Unix, AS/400, Novell NetWare, Työryhmä-Windows, LAN Manager...)
- Mitä voidaan ja halutaan korvata Windows NT-verkolla
- Mistä halutaan lopullisesti eroon
- Miten mikrotuki on nyt hoidettu ja miten sen tulisi olla hoidettu
- Käyttäjien tyytyväisyys ja tietotarpeet
- Koulutus.

Mikä olisi **tavoitetila**, johon halutaan:

- Käyttäjien ja yrityksen **todelliset** tarpeet
- Oheislaitteet ja sovellusohjelmat
- Tiedonsaanti ja -siirto sekä pääteyhteydet
- Sisäinen ja ulkoinen viestintä (ja mitä se saa maksaa)
- Tiedonhallinta ja tietoturvallisuus: käyttäjätunnukset ja -oikeudet, fyysiset suojaukset, laitetilat, kirjoittimet (ja tietoturvallisuus suojausjärjestelmineen ja varalaitteistoineen saa maksaa)
- Tulostus: erikoislomakkeet, laskutulostus, massatulostus...
- Erilliset testausympäristöt
- Organisointi ja vastuualueet.

Mitä **jatkossa**? Verkon kanssa on elettävä vuosia, joten:

- Pitkän tähtäimen suunnitelmat (**PTS**): siirretäänkö Windows NT-ympäristöön myös operatiiviset sovellukset (tietokantapalvelimet)

- Tulevat tarpeet ja alan kehitys: otetaanko käyttöön Windows NT- vai Windows 95 -työasemat, tiedonsiirtokapasiteetin tarpeen kasvamisen huomioiminen verkossa, multimedia, ulkoiset yhteydet...

- Käyttäjä/laitemäärien muutokset

- Tuki ja ylläpito sekä kehitys jatkossa. Kenellä on esimerkiksi oikeus lisätä ja muuttaa käyttäjätunnuksia, miten **Help Desk** järjestetään jne. Jos et huolehdi näistä asioista ajoissa, ne jäävät järjestelmän käyttöönotosta vastanneelle yksikölle

- Budjetointi, kustannukset...

Kun nämä ajatukset on hahmoteltu, niin ennenkuin suinpäin ryhdytään asentamaan palvelimia, kannattaa **suunnitella** verkon käyttö:

- Palvelimet ja resurssit: niiden nimet, oikeudet, asennusmetelmät ja -standardit, hakemistorakenteet, varmistukset, osoitteet...

- Käyttäjämäärät palvelinta kohti ja palvelinten kuormitus; käyttäjien ryhmittely, toimialuemallit...

- Suojaukset ja varmuuskopiointi: menetelmät, rutiinit, tallennuspaikat...

- Oheislaitteet: standardointi, käyttöoikeudet, suojaaminen...

Toimialuemallien suunnittelussa tulee huomioida:

- Kirjoittautuvatko käyttäjät useammasta toimialueesta päätoimialueelle (*Master Domain*) - jos, niin yhden toimialueen malli ei tule kyseeseen

- Työasemien ja palvelimien välillä voi käyttää reitittimiä ja WAN-yhteydet voivat olla globaaleita

- **Luottava** (*Trusting*) toimialue sisältää käyttäjien tarvitsemat resurs-sit; **luotettu** (*Trusted*) sisältää käyttäjätunnukset asetuksineen

- Luottosuhteita ei voi välittää toimialueiden välillä

- Yksittäinen toimialue voi sisältää 26000 tietokone- ja käyttäjätunnusta

- Siirtymistä Windows NT 5.0:een tulee helpottamaan käyttäjien ryhmittely yleisiin ryhmiin (*Global Groups*).

Testaus

Tee ensin testiverkko, jossa on vaikkapa kolme palvelinta. Ne voisivat muodostaa **kaksi toimialuetta**, jossa toisessa on **kaksi palvelinta** (PDC ja BDC). Lisäksi tarvitaan ainakin yksi työasema; se voi olla Windows NT-työasema, jossa MS-DOS:in lisäksi on Työryhmä-Windows ja Windows 95 (jos näitä on organisaatiossa käytössä).

Tällöin voit testata käytännössä toimialueen muodostamisen ja luottosuhteiden määrittelyn kahden toimialueen välillä. Opiskele myös palvelimien roolin vaihtaminen.

Huomioitavaa:

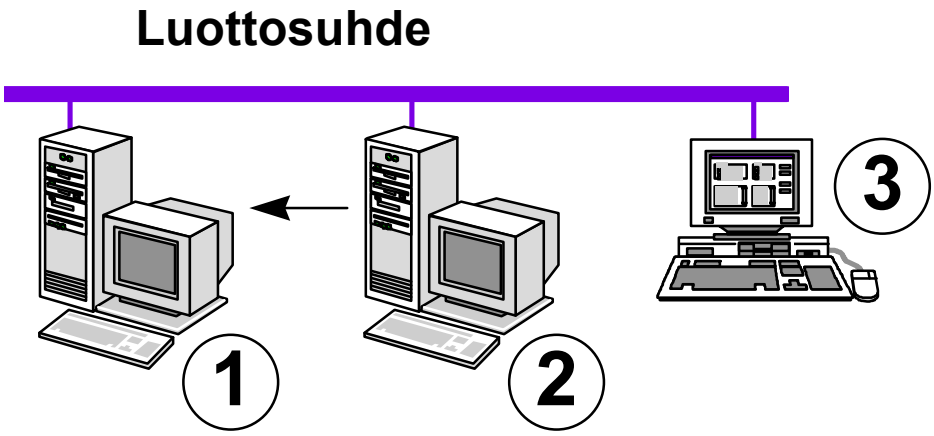
- Tällaisiksi testipalvelimiksi riittää esimerkiksi i486/66 32 Mt keskusmuistilla. 500 Mt - 1 Gt kiintolevy on suositeltava; levy(t) voivat olla IDE-tyyppisiä, joskin SCSI on suositeltavin. Ainakin jossakin palvelimista tai työasemassa tulisi olla CD-ROM; se voi olla ATAPI-tyyppinenkin. Näytönohjaimeksi riittää perus-VGA 1 Mt muistilla. Myös hiiri ja verkkokortti tarvitaan.

- Asenna palvelimiin NT siten, että osioit NT:n omalle osiolleen (esimerkiksi 300 Mt) ja loput jätät muuhun käyttöön.

- Asenna etäkäyttöpalvelin ja modeemi palvelimeen (9600 bps riittää harjoitteluun)

- Asenna työasemaan modeemi etäkäytön opiskelua varten (9600 bps riittää tässäkin harjoitteluun)
- Asenna palvelimeen jokin kirjoitin; esimerkiksi vanhempi LaserJet käy mainiosti
- Asenna kahteen palvelimeen WINS ja muodosta niiden välille replikointi
- Asenna yhteen NT-palvelimeen IIS ja DHCP. Opiskele näiden konfigurointi
- Määrittele DHCP:n jakama alue (*Scope*) siten, että annat asetukseksi **044 WINS/NBNS Servers** PDC:n osoitteen, jossa DHCP-palvelin toimii. Lisäksi on määriteltävä **046 WINS/NBT Node Type** esimerkiksi **0x08** (H-node)
- Tutustu isäntätiedostoihin (HOSTS, LMHOSTS) ja opiskeli nimiselvitysmenetelmät
- Kokeile eri palveluiden toiminnat myös mahdollisessa reititinverkossasi. Tee tarvittavat **HOSTS**- ja **LMHOSTS**-asetustiedostot.
- Testaa myös mahdollinen **Gateway Service for Novell Netware**
- Harjoittele järjestelmän elvytys.

Tässä esimerkin harjoitusympäristössä on tehty **VARASTO**-toimialueen PDC multibootiksi siten, että asennetaan samaan mikroon kaksi kertaa NT-palvelin, mutta eri hakemistoihin; toinen käynnistys on **HALLINTO**-toimialueen BDC ja toinen **VARASTO**-toimialueen PDC.

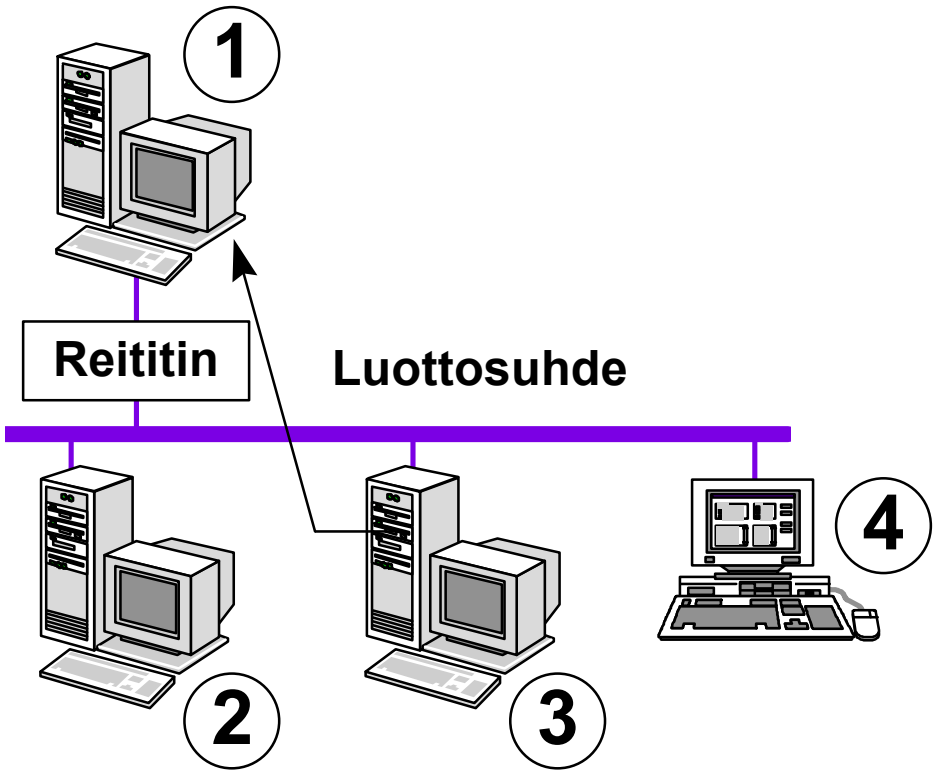


1) Palvelin H1, toimialue HALLINTO (PDC), C: 300 Mt (NTFS), D: loput, esim. 700 Mt (NTFS). Jaettuja resursseja esimerkiksi: \USERS, \OHJELMAT, CD-ROM, kirjoitin, IIS, DHCP, WINS, RAS

2) Palvelin V1, toimialue VARASTO (PDC), multiboot, myös HALLINTO-toimialueen palvelin H2 (BDC). Yksisuuntainen luottosuhde HALLINTO-toimialueeseen. C: 300 Mt (NTFS), D: loput (NTFS). Jaettuja resursseja esimerkiksi: \USERS, \OHJELMAT, CD-ROM, kirjoitin

3) Multiboot-työasema: Windows NT, Työryhmä-Windows (WfW), Windows95, palvelimen etähallintaohjelmat, toimialue VARASTO (C: FAT, D: NTFS)

Toisessa esimerkissa palvelimet ovat erillisiä ja lisämaustetta tuo **HALLINTO**-toimialueen BDC, joka on tuotu reitittimen taakse saman toimialueen PDC:stä. Tämä saattaa olla tilanne, kun sovelletaan vaikkapa **Master Domain** -toimialuemallia maantieteellisesti laajassa verkossa.



1) Palvelin H, toimialue HALLINTO (PDC)

2) Palvelin H2, toimialue HALLINTO (BDC), C: 300 Mt (NTFS), D: loput (NTFS). Jaettuja resursseja esimerkiksi: \USERS, \OHJELMAT, CD-ROM, kirjoitin, lisäksi asennettuna IIS, DHCP, WINS, RAS

3) Palvelin V1, toimialue VARASTO (PDC), yksisuuntainen luottosuhde HALLINTO-toimialueeseen, C: 300 Mt (NTFS), D: loput (NTFS), jaettuja resursseja esimerkiksi: \USERS, \OHJELMAT, CD-ROM, kirjoitin

4) Multiboot-työasema: Windows NT, Työryhmä-Windows (WfW), Windows95, toimialue VARASTO, C: FAT, D: NTFS

Pyri myös tutustumaan paitsi Windows NT, myös Windows 95 -työaseman, konfigurointiin sekä toimialueen käyttäjien määrittelyyn työasemassa:

- Jos käytät TCP/IP-protokollaa, tutustu sen asetuksiin eri työasemissa ja palvelimissa. Käytä myös mahdollisuuksien mukaan WINS- ja DHCP-palveluita

- Käytä verkkoa hyväksesi mahdollisimman paljon itse asennuksessa. Esimerkiksi asennukset voi hoitaa hyvin pitkälle verkkokäynnistyslevykkeen ja verkkoon jaetun CD-ROM:in avulla. Kirjoittava CD-ROM saattaa osoittautua hyödylliseksi arkistoitaessa ja/tai jaettaessa sovelluksia

- Itse palvelimissa on suositeltavaa käyttää nauhavarmistimia ja CD-ROM-asemia. Palvelimien laitteiston tulisi toki muutenkin olla mitoitettu käytön mukaan; PCI-verkkokortit, SCSI-kiintolevyjärjestelmät (RAID 5) ja riittävästi keskusmuistia (64 Mt tai enemmän) jne.

- Luo toimialueet, toimialueen käyttäjäryhmät ja yksittäiset käyttäjät. Pyri käyttäjäryhmissä alkuvaiheessa tukeutumaan NT:n valmiisiin käyttäjäryhmiin

- Määrittele ja luo palvelinten ja työasemien hakemistorakenteet ja työasemien asennusrutiinit. Standardoi - mikä on käytettävä työasemaympäristö, mitä sovelluksia käytetään jne

- Asenna ja testaa käytettävät sovellukset. Muista testata riittävän isolla samanaikaisella käyttäjämäärällä!

- Muista käyttäjien osasllistuminen suunnittelun ja testaukseen!

- Toteuta tulostusjärjestelyt. Windows 95 ja NT tukee verkkotulostimia (HP JetDirect jne) sekä NT-palvelin tukee TCP/IP-tulostusta (LPR/LPD)

- Etäkäyttäjien tuki - miten RAS (Remote Access Service)-palvelu toteutetaan, kuka saa etäkäyttää verkkoa, onko oikeus vain RAS-palvelimeen vai koko verkkoon jne

- Sähköpostin ulkoiset yhteydet - mitä halutaan, kuka ylläpitää

- Virustorjuntamenettelyt ja -sopimukset

- Vakuutukset

- Muista varalaitteistojen merkitys! Älä unohda myöskään katastrofisuunnitelmaa. Hanki riittävän suurikapasiteettiset UPS-laitteet

- Suunnittele varmistusmenettely, myös työasemien osalta. Älä unohda kirjoittavien CD-ROM:ien käyttömahdollisuutta arkistoinnissa. Testaa palautukset.

Tee kokemusten perusteella projekti-/toimeenpanosuunnitelma.

Standardointi

Standardoinnin avulla luodaan yhteiset pelisäännöt. Tällöin pystytään erilaiset vikatilanteet paikantamaan nopeammin ja mikrotukikin toimii tehokkaammin. Käyttäjät eivät ylläty "vieraalla" työasemalla ja saavat käyttöönsä haluamansa palvelut kautta verkon. Verkon hallinta helpottuu. Samalla kustannuksetkin pienenevät, mikä onkin koko standardoinnin lopullinen tarkoitus.

Standardoinnin oleellinen osa on normaaleiden, usein tapahtuvien toimintojen rutinointi. Pyri tekemään rutiinit eri toimintoja varten:

- Käyttäjätunnukset
- Käyttäjien lisääminen / siirtäminen /poistaminen
- Käyttäjien koulutus ja koulutuksen järjestäminen
- Koulutusmateriaalin tilaaminen ja jakelu
- Tiedottaminen
- Mikrotuen toiminta (Help Desk, vierihoito...)
- Laitteistojen nimeäminen ja konfigurointi
- Työasemien ja palvelmien hankinta, asennus ja käyttöönotto
- Ohjelmistojen hankinta, päivitys ja lisensointi
- Verkon valvonta
- Etäkäyttömenetelmät ja -oikeudet

- Sähköpostitunnukset
- Henkilökunnan omien mikrojen ja ohjelmistojen hankinta; jonkun nekin on hankittava

Dokumentoi ja tiedota eri menettelytavoista.

Käyttöönotto

Kun suunnitelmat ja standardit ovat valmiina, voidaan toteuttaa suunnitelman mukaisesti verkon käyttöönotto. Yleensä tällaiset käyttöönotot ovat edenneet organisaatioyksiköittäin - myös yksiköiden maantieteellisen sijainti vaikuttaa asiaan.

Muista riittävän tiedottamisen merkitys! Älä kuitenkaan kerro käyttäjille viimeisen Service Packin korjauksista tai muutakaan *TechnoJargonia*, vaan käyttäjiä todella koskevista asioista; esimerkiksi kirjoittimien uusista sijoitteluista, tulostusmenettelyistä, jonojen nimistä jne.

Tiedottamisessa voi käyttää mainiosti hyväksi sisäistä WWW-palvelinta.

Muista koulutus: käyttäjillä tulisi olla perus- ja jatkokoulutusta sekä selkeä koulutusohjelma. Koulutuksesta tulisi saada palautetta!

Tunnin/kahden tietoiskut ovat osoittautuneet usein hyödyllisiksi. Tilanteen pitää olla vapaamuotoinen ja käyttäjiltä tulisi saada palautetta - keskustelumuotoisesti. Vältä tilannetta, jossa "sanellaan" tulevat ratkaisut. Älä lupaa asioita, joita ei pystytä toteuttamaan.

Muista käyttöönotossa seuraavien menetelmien hyödyntämismahdollisuudet:

- Systems Management Server
- Vakiolevyasematunnukset
- Logon-skriptit
- Käyttäjäprofiilit (Windows NT, Windows 95)
- Komentojonot (BAT, CMD)

Muista myös seuraavat:

- TCP/IP:n hallinta - IP-osoitteet ja nimiselvitys: DHCP, DNS, HOSTS, WINS, LMHOSTS...
- Verkkokirjoittimet)
- Internet Information Server

Dokumentoi tehdyt ratkaisut.

Jälkihoito

Muista varmistusten tärkeys ja jatkuva verkon toiminnan seuranta. Muista myös ylläpitää verkon asennuksen yhteydessä syntyneitä dokumentteja.

Ongelmatilanteiden hoitoon olisi syytä tehdä **rutiinit** - ja kertoa käyttäjiä koskevat myös heille. Tällaisia rutiineja voivat olla:

- Varapalvelinten asennus/käyttöönotto
- Virusepidemian hoitaminen
- TCP/IP-osoitteiden hallinta
- Käyttäjien hallinta
- Kirjoittimien hallinta
- Lisenssien hallinta ja kustannusten "vierittäminen".

Käyttäjiä ei muutenkaan pidä unohtaa:

- Standardointi
- Ohjeistus
- Tuki ja valvonta
- Koulutus- ja käyttöönottosuunnittelu
- Työasemakoulutus
- Windows-koulutus
- Sovelluskoulutus
- Internet-koulutus
- Sähköpostikoulutus.

Eikä **tuen** eli esimerkiksi **laitetoimittajien** apua:

- Perinteiset edellytykset
- Huolto
- Tekninen tuki

- Suhteet päämiehiin

Huolehdi myös (muiden) **tukihenkilöiden** vireydestä:

- Koulutus
- Ohjeistuksen saatavuus ja ylläpito
- Tarvittaessa saatavat lisäresurssit.

Muista, että kerran rakennettua verkkoratkaisua saattaa olla hankala muuttaa myöhemmin.

Windows NT 5.0

Siirtymistä Windows NT 5.0:aan tulee todennäköisesti helpottamaan seuraavat Windows NT 4.0-ympäristön seikat:

- Master Domain-mallin käyttäminen ja käyttäjien ryhmittely yleisiin ryhmiin (Global Group)
- DNS-nimipalvelun käyttäminen ja nimeämisen suunnittelu.

Siirtymisvaiheessa suurin työ tullee olemaan Active Directoryn rakentaminen, ja siihen Microsoft on tuomassa työkaluja.

Windows NT 5.0 tuo mukanaan todennäköisesti ainakin seuraavat ominaisuudet:

- **Active Directory** - nimeämiskäytännöt tulevat muuttumaan CCITT X.500-hakemistostandardin mukaisiksi, protokolla on LDAP (*Lightweight Directory Access Protocol*) ja myös DNS on käytössä. Niinpä esimerkiksi DIT:n (*Directory Information Tree*) käyttäjätunnus voi olla CN=Jyrki Kivimaki,OU=Varasto,O=Fishware,C=FI jossa CN on nimi (*Common Name*), OU on organisaatioyksikkö (*Organization Unit*), O on organisaatio (*Organization*) ja C on maa (*Country*). Hakemisto on myös laajennettavissa, esimerkiksi voidaan lisätä puhelinnumerot jne

- **Distributed File System** (DFS) tuo Active Directoryn mukana mielenkiintoisia piirteitä. Esimerkiksi UNC-nimet (*Universal Naming Convention*) voivat viitata **toimialueeseen**, esimerkiksi **\\FISHWARE\DATA**. Samoin kotihakemistot voivat viitata varsinaiseen hakemistoon, esimerkiksi kirjauskomentojonoon voidaan lisätä komento **NET USE H: \\Server1\Users\PerttiM**. Yksi jakonimi voi myös käsittää jakonimiä ja hakemistoja muistakin palvelimista. DFS-asiakasohjelmisto on mukana Windows NT 4.0-työasemassa. DFS:n avulla voi myös ohjata yhden jakonimen useampaan palvelimeen; tällä saadaan lisää vikasietoisuuspiirteitä

- **PDC** (*Primary Domain Controller*) ja **BDC** (*Backup Domain Controller*) katoavat, on vain DC (*Domain Controller*), jossa PDC:tä voidaan ajaa palveluna. Esimerkiksi käyttäjien asetuksia voi muuttaa milloin vaan, DC:t synkroinoivat keskenään käyttäjätietokannan muutokset (luottosuhteet ovat edelleen olemassa, mutta ne mahdollistavat hierarkiset toimialuemallit).

Ylläpito

Ylläpidon voisi sanoa tarkoittavan Windows NT-ympäristön jatkuvaa valvontaa ja hallintaa. Lähiverkkoon tai internetiin kytketty Windows NT *ei* ole yhden mikron *viidessä pienessä minuutissa* hoidettu PC - mikä onkin jo useimmille tehokäyttäjille tuttu asia.

Tehtäviin voidaan katsoa kuuluvan:

- Käyttäjien hallinta
- Käyttäjien profiilien määrittely ja hallinta
- Palvelimien ja niiden resurssien hallinta
- Kiintolevyjen ja levytilan hallinta
- Tapahtumien valvonta
- Hakemistokopioinnin valvominen
- Valvontatyökalujen käyttö
- Apuohjelmien käyttö rutiinien apuna

- Varmistusmenetelmät
- Ohjelmistojen asennukset ja päivitykset
- Virustorjunta.

Joitakin näistä asioista on jo sivuttu aiemmin tässä kirjassa.

Levytilan hallinta

Levytilan hallintaan ei Windows NT:n mukana toistaiseksti tule mitään työkaluja. Resource Kitin **DIRUSE**-apuohjelmalla voi valvoa, mutta ei rajoittaa levytilan käyttöä.

Seuraavia menetelmiä voi noudattaa:

- Luo eri levyosiot järjestelmälevylle ja käyttäjien kotihakemistoille
- Käytä tarvittaessa NTFS:n pakkausominaisuuksia
- Käytä Performance Monitorin hälytyksiä levytilan valvontaan
- Käytä Resource Kitin DIRUSE-apuohjelmaa levytilan valvonnassa
- Hanki erillinen levytilan hallintaohjelma, esimerkiksi:
  - **Quota Server**, **http://northern.se**
  - **Quota Advisor**, **http://www.wquinn.com**
  - **Quota Manager**, **http://ntpsoftware.com**.

Varmuuskopiointi

Yhtä tärkeä kuin palvelimen kiintolevy on varmuuskopio kiintolevyn tiedostoista. Joitakin nyrkkisääntöjä varmuuskopioinnista:

- Älä jätä varmuuskopioita varmuuskopiointilaitteeseen, josta ne voidaan ottaa luvatta
- Salakirjoita varmuuskopiot, jos tiedot ovat salaisia
- Käytä useita varmuuskopionauhoja vuorotellen ja säilytä pysyviä varmuuskopioita turvallisissa paikoissa jossakin muualla kuin yrityksen omissa tiloissa
- Varmista tarvittaessa varmuuskopioiden turvallisuus matkalla säilytyspaikkaan
- Dokumentoi ja luetteloi kaikki varmuuskopiot varkauden varalta
- Tarkista säännöllisin väliajoin varmuuskopioiden kunto ja tietojen palauttaminen
- Varmuuskopioi myös työasemilla olevat tiedostot.

Varmuuskopiointi komentojonojen avulla

Yhden tai useamman levyaseman säännöllistä varmuuskopiointia varten voi kirjoittaa komentojonon (CMD tai BAT). Syntaksi on:

NTBACKUP [TOIMINTO POLUT [VALITSIMET]]

Parametrit:

toiminto **Backup** - suoritetaan varmistus

polut Levyasematunnus: A: B: C: ... Z: ja mahdollinen **\hakemisto**

Valitsimet:

/A	**A**[ppend] jos haluat liittää uudet sarjat vanhojen perään
/V	**V**[erify] jos haluat varmistaa varmuuskopioinnin
/R	**R**[estrict] jos haluat rajoittaa käyttöoikeuden
/D	**D**[escription] kuvausteksti lainausmerkeissä
/B	Paikallisen rekisterin kopiointi
/Hc:on tai **/Hc:off**	Laitteistopohjainen pakkaus (*Hardware Compression*)
/T	**T**[ype] eli varmistustyyppi: **Normal**, **Copy**, **Incremental**, **Differential**, **Daily**
/L	**L**[og] eli lokivalinnat = lokitiedoston nimi lainausmerkeissä [Vain_poikkeustapahtumat]
/E	**/E**[xceptions] vain poikkeustapahtumien tallennus
/Tape:n	Nauha-aseman numero **0 - 9**.

Jos et määritä **Append**-vaihtoehtoa (**/A**), varmistusohjelma käyttää nauhan uudelleen ja **korvaa vanhat tiedot**. Jos annat **/A**, varmistusohjelma liittää uudet varmuuskopiosarjat vanhojen perään. Jos olet valinnut useita levyasemia, eikä **/A**-valintaa ole tehty, varmistusohjelma korvaa nauhan aiemman sisällön ensimmäisen valitun aseman varmuuskopioilla ja liittää seuraavien asemien varmuuskopiot niiden perään.

Jos teet **BACKUP.BAT**:in, jossa on seuraava komento:

```
NTBACKUP BACKUP C:\ D:\ E:\ /V /D "DAILY FULL" /B /HC:ON /T NORMAL  /L "C:\USERS\DEFAULT\DAILYFUL.TXT" /TAPE:0
```

Niin se varmistaa C:-, D:- ja E:-aseman ja rekisterin normaalivarmistuksena, tarkistaa varmistuksen, tekee kuvauksen, käyttää laitepohjaista pakkausta ja kirjoittaa lokin.

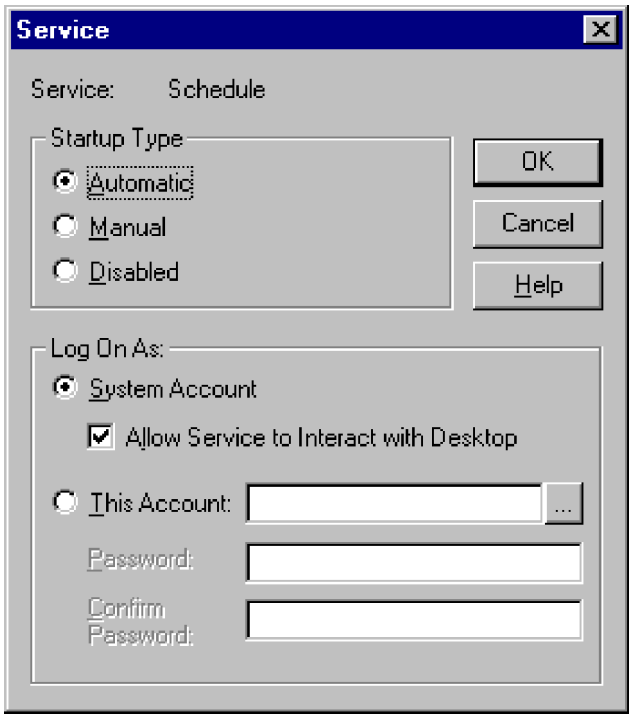
Komentojono loppuun voisi lisätä komennon

NTBACKUP /EJECT

joka poistaa nauhan asemasta.

Varmuuskopioinnin ajastaminen

AT-komentoa voit käyttää varmistuksen ajastamiseen. Tällöin **Schedule**-palvelun pitää olla käynnissä; käynnistys tehdään Ohjauspaneelista Services-kuvakkeella käynnistämällä **Schedule**-palvelu. Määrittele käynnistystyypiksi **Automatic** sekä anna lupa tuoda ilmoitukset näyttöön **Allow Service to Interact with Desktop**.



Voit käynnistää sen myös komentoriviltä komennolla **NET START SCHEDULE** sekä suomen- että englanninkielisissä versioissa. Komennolla **NET START**, näet mitä palveluja on käynnissä.

AT-komennon syntaksi on:

AT [\\TIETOKONENIMI] [[TUNNUS] [/DELETE [/YES]]
AT [\\TIETOKONENIMI] AIKA [/INTERACTIVE] [/EVERY:PÄIVÄMÄÄRÄ[,...] | /NEXT:PÄIVÄMÄÄRÄ[,...] "KOMENTO"

Ilman parametreja käytetty AT-komento antaa luettelon ajastetuista komennoista.

Parametrit ovat seuraavat:

\\nimi	Määrittää etäkoneen. Jos tätä parametria ei anneta, komennot ajastetaan suoritettaviksi paikallisella tietokoneella
tunnus	Ajastetun komennon tunnusnumero (ID)
/delete	Peruuttaa ajastetun komennon. Jos tunnusta ei anneta, kaikki tietokoneen ajastetut komennot peruutetaan (myös **/D**)
/yes	Antaa myönteisen vastauksen kaikkiin kysymyksiin, joita järjestelmä esittää ajastettujen tapahtumien poistamisen yhteydessä (myös **/Y**)
/interactive	Jos ajastettu komento odottaa esimerkiksi käyttäjän näppäimen painallusta, tällä valitsimella mahdollistetaan vuorovaikutteisuus. Tämä on tärkeä valitsin esimerkiksi ajastettaessa virustorjunta- tai varmistusohjelmia, koska ne saattavat esimerkiksi odottaa **OK**:n painallusta tms. Ilman tätä valitsinta sovellus saattaa vaikuttaa jääneen jumiin
aika	Määrittää komennon suoritusajan. Aika annetaan 24-tuntisessa muodossa tunnit.minuutit (00.00 [keskiyö] - 23.59)
/every:päivämäärä[,...]	Suorittaa komennon jokaisena annettuna viikon tai kuukauden päivänä (esimerkiksi joka torstai tai kuukauden kolmantena päivänä). Anna argumentiksi päivämäärä vähintään yksi viikonpäivä (ma, ti, ke to, pe, la, su) tai kuukaudenpäivä

(numeroilla 1 - 31). Erota argumentit pilkulla. Jos et anna päivämääräparametria, oletusarvona on kuukauden kuluva päivä. Englanninkielisessä versiossa vastaavat päivät ovat m, t, w, th, f, s ja su

/next:päivämäärä[,...] Suorittaa määritetyn komennon seuraavana annettuna päivänä (esimerkiksi seuraavana torstaina). Anna argumentiksi päivämäärä vähintään yksi viikonpäivä (ma, ti, ke, to, pe, la, su) tai kuukaudenpäivä (numeroilla 1 - 31). Erota argumentit pilkuilla; jos et anna päivämääräparametria, oletusarvona on nykyisen kuukauden kuluva päivä

"**komento**" Suoritettava Windows NT:n komento, ohjelmatiedosto (tunnisteen on oltava .EXE tai .COM) tai komentojonotiedosto (tiedoston tunniste .BAT tai .CMD). Jos komennon argumentiksi on annettava polku, kirjoita **absoluuttinen polku** eli koko polku aseman tunnuksesta alkaen. Jos suoritettava komento on etäkoneessa, anna palvelimen nimi ja jakonimi etäkoneen aseman tunnuksen sijasta. Voit kirjoittaa komennon myös lainausmerkkeihin sekä komentorivillä että komentojonotiedostossa.

Halutessasi tarkastella ajoitettuja komentoja, voit tehdä sen antamalla AT-komennon. Jos annat AT-komennon ilman valitsimia, esiin tulee seuraavanlainen näyttö:

Status ID	Day	Time	Command Line
0	Today	18:00	viruscan.bat
1	Today	18:50	NET SEND * VARMISTUS ALKAA - POISTU VERKOSTA!
2	Today	19:00	varmista.bat

Kun annat komennon tunnusnumeron, näyttöön tulee seuraavanlaisia tietoja yhdestä komennosta tai ohjelmasta:

Task ID: **1**
Status: **OK**
Schedule: **Today**
Time of day: **18:50**
Interactive: **No**
Command: **NET SEND * VARMISTUS ALKAA - POISTU VERKOSTA!**

AT-komennolla ajastetut komennot suoritetaan taustalla, joten niistä ei tule mitään ilmoituksia näyttöön. Voit ohjata suoritettavan komennon tulosteet tiedostoon käyttämällä uudelleenohjausmerkkiä (esimerkiksi tiedot hakemistojen käyttöasteesta **AT 19:00 "DIRUSE C:\USERS /Q:20 > LISTA.TXT"**). Jos ohjaat tulosteet tiedostoon, kirjoita ajastettavan komennon nimi lainausmerkkeihin. **DIRUSE** on hakemistojen tilankäytön seurantaohjelma, joka tulee Resource Kitin mukana.

Huomaa:

- Jos muutat välillä kellonaikaa, synkronoi ajastin muutetun ajan suhteen kirjoittamalla AT-komento ilman valitsimia!
- Jos suoritettavassa komennossa on valitsimia, joita myös AT-komento käyttää, argumentti on ehdottomasti kirjoitettava lainausmerkkeihin
- Ajastetut komennot tallentuvat rekisteriin, joten ne eivät katoa, vaikka ajoituspalvelu käynnistetään uudelleen.
- Oletuksena vain Administrators-ryhmän jäsenet voivat ajastaa komentoja. Oikeus voidaan antaa lisäksi järjestelmätason käyttäjäryhmille (mutta ei Everyone-ryhmälle) **Submit Control**-asetuksen arvolla **1**:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\Lsa**
Nimi	**Submit Control**
Tyyppi	**REG_DWORD**

Arvo	**1**

Esimerkkejä:

- Saat luettelon **SERVER4**-palvelimen ajastetuista komennoista kirjoittamalla **AT \\SERVER4**
- Voit peruuttaa kaikki ajastetut komennot komennolla **AT /D**.
- Voit peruuttaa ajastetun komennon ID-nro **2** NT-koneessa **V2** komennolla **AT \\V2 2 /D**.

Anna komentorivillä komento:

AT 04:00 /EVERY:T,W,Th,F,Sa /INTERACTIVE "C:\BATCH\BACKUP.BAT"

Niin saat ajastettuna varmistuksen ajettavaksi tiistai-lauantai klo 04. (**Backup.bat** on esitetty aiemmin, ks. Varmistukopiointi komentojonojen avulla).

Resource Kitissä tulee mukana komentojen ajastukseen tarkoitettu **Command Scheduler** (WINAT.EXE), jolla voit myös tehdä saman.

SQL Serverin varmuuskopioiminen

SQL Serverin (tai minkä tahansa palvelinsovelluksen tietokantojen) varmistamisen voit tehdä seuraavanlaisella komentojonolla:

```
NET STOP MSSQLSRV
CALL BACKUP.BAT
NET START MSSQLSRV
```

Esimerkissä **NET STOP**- ja **NET START**-komennot käynnistävät ja sammuttavat a.o. palvelun. **CALL**-komento kutsuu tarvittavaa nauhavarmistuksen suorittavaa komentojonoa.

Avointen tiedostojen varmistaminen

Avointen tiedostojen varmistaminen on perinteinen ongelma. Avattua tiedostoa ei yksinkertaisesti *voi* varmistaa, mutta NT Backup odottaa oletuksena **30** sekuntia tiedoston sulkeutumista. Asetukset ovat rekisterissä:

Polku	**HKEY_CURRENT_USER\SOFTWARE**
Avain	**\Microsoft\NTBackup\User Interface**
Nimi	**Skip open files**
Tyyppi	**REG_SZ**
Arvo	**0 - älä ohita, odotetaan, kunnes tiedosto suljetaan (oletus)** **1 - ohitetaan kirjoitusta varten avatut tiedostot automaattisesti** **2 - odotetaan Wait time-mukaisen ajan**

Polku	**HKEY_CURRENT_USER\SOFTWARE**
Avain	**\Microsoft\NTBackup\User Interface**
Nimi	**Wait time**
Tyyppi	**REG_SZ**
Arvo	**30 sekuntia (oletus), maksimiarvo on 65535 sekuntia**

Järjestelmän palauttaminen nauhalta

Seuraavaksi yksi menetelmä Windows NT:n palauttamiseksi nauhalta:

1) Vaihda toimiva kiintolevy hajonneen tilalle

2) Asenna uudelleen Windows NT (työasemakin käy) esimerkiksi **C:\NT**-nimiseen hakemistoon (tai mihin tahansa, jossa ei varmasti ole hajonnut NT-asennus). Asenna vain välttämättömimmät (työasema-asennus ei vaadi verkkoa), mutta asenna nauhalaitteen laiteohjain

3) Palauta edellinen täydellinen varmistus nauhalta, palauta myös rekisteri valinnalla **Restore Local Registry**. Palauta myös vähintään muut järjestelmän tiedostot

4) Korjaa **BOOT.INI**-tiedoston asetuksia niin, että se käynnistää NT:n hajonneen NT-asennuksen hakemistosta (oletuksena **C:\WINNT**)ja käynnistä NT-palvelin uudelleen

5) Kaiken pitäisi nyt toimia - ainakin siten, kuin ne edellisillä varmistuksilla olivat.

Levyjen hallinta

Windows NT 4.0 Server -palvelinversion Disk Administratorissa on seuraavat vikasietoisuuslaajennukset (*Fault Tolerancy*) verrattuna **Windows NT 4.0 Workstation**-työaseman levynhallintaan:

- Peilausparien luonti (*Mirrored Disk*)
- Raitasarjojen (rinnakkaisosioiden) pariteettitarkistus (*Stripe Set with Parity*).

Stripe Set with Parity

Tämä toiminto on käytettävissä vain Windows NT -palvelimien Disk Administratorissa.

Voit luoda **pariteettitarkistettuja raitasarjoja** (*Stripe Set with Parity*) yhdistämällä erikokoisia vapaan tilan alueita 2 - 32 levyltä **yhdeksi loogiseksi levyksi**. Vikasietoisuutta voidaan parantaa raitasarjojen avulla **tarkistamalla levyn pariteettitiedot**; nämä tiedot levitetään tasaisesti eri levyille. Niinpä pariteettitarkistetuissa raitasarjoissa on **yksi ylimääräinen pariteettitarkistus** ja näitä ylimääräisiä pariteettitietoja varten on käytettävä **kahden levyn sijasta vähintään kolmea levyä**.

Pariteettitarkistuksia sijoitetaan eri puolille osioita tietojen siirtokuormituksen tasapainottamiseksi - näin saavutetaan yhtä täydellinen suojaus kuin levyn peilaamisella, mutta tiedoista saadaan samalla ylimääräinen kopio yhden lisälevyn hinnalla. Laitteistopohjaisesta menetelmästä

käytetään tavallisesti termiä **RAID 5**.

Pariteettitarkistettua raitasarjaa käytettäessä levyvirheen jälkeinen tietojen palauttaminen vie kuitenkin enemmän aikaa kuin peilauspareja käytettäessä.

Pariteettitarkistetun raitasarjan luominen tehdään seuraavasti:

1) Valitse vähintään **kolme** vapaan tilan (Free Space) aluetta 3 - 32 kiintolevyltä valitsemalla ensimmäiseltä levyltä ensimmäinen vapaa alue ja painamalla **Ctrl**-näppäintä; valitse sitten lisäalue kultakin muulta kiintolevyltä

2) Valitse **Fault Tolerance** | **Create Stripe Set with Parity**. Levynhallinta näyttää pariteettitarkistetun raitasarjan vähimmäis- ja enimmäiskoon. Anna luotavan raitasarjan koko

3) Valitse **OK**.

Levynhallinta jakaa kokonaistilan levyjen määrällä, joten se luo valituille levyille samankokoiset alustamattomat osiot ja asettaa yhden levyaseman kirjaimen osioryhmälle, joka muodostaa pariteettitarkistetun raitasarjan.

Kun haluat käyttää pariteettitarkistetun raitasarjan tilan muihin tarkoituksiin, ota ensin varmuuskopiot ja valitse sitten **Partition** | **Delete**. Kun poistat raitasarjan, kaikki sen sisältämät tiedot häviävät.

Mirroring

Levyn peilaaminen (*Mirroring*) suojaa levyn osiota **levyvirheiltä** ja laitteistosta riippuen myös mahdolliselta **levyohjainvirheeltä**, koska se pitää ylimääräistä kopiota tiedoista toisella levyllä. Laitteistopohjaisesta menetelmästä käytetään tavallisesti termiä **RAID 1**.

Jos peilattu osio vaurioituu, peilaus on katkaistava. Tällöin jäljellä olevasta **toissijaisesta** osiosta tulee erillinen levy, jolla on oma aseman kirjain. Tästä levystä tulee **pääosio**. Voit määrittää sille uuden peilauksen, jonka vapaan tilan määrä on yhtä suuri tai suurempi kuin peilattavan osion varaama tila.

Peilauspari (**Mirror Set**) luodaan kopioimalla osio toiselle levylle. Kum-

mankin osion aseman kirjaimena on sama kirjain. Mikä tahansa osio (myös järjestelmä- ja käynnistysosio) voidaan peilata toiseen, toisella levyllä olevaan, vähintään samankokoiseen osioon. Käytettävän levyn ohjaimen ei tarvitse olla sama; itse asiassa käyttämällä kahta levyohjainta parannetaan turvallisuutta vielä lisää - tällöin käytettän termiä *Disk Duplexing*. Peilaus varaa aina toisen levyn kapasiteetin; eli jos peilaat kahta 4 Gt:n kiintolevyä, käytettävissäsi on vain 4 Gt:n verran levytilaa.

Peilausparin luominen tehdään seuraavasti:

1) Valitse ensimmäinen alue ja paina **Ctrl**-näppäintä; valitse sitten toinen alue, jonka on oltava suurempi tai yhtäsuuri kuin ensimmäinen alue ja lisäksi vapaa (Free Space)

2) Valitse **Fault Tolerance** | **Establish Mirror**

Levynhallinta luo vapaaseen tilaan samankokoisen osion peilausta varten ja asettaa peilausparin aseman kirjaimen.

Kun haluat käyttää peilausparin tilan muihin tarkoituksiin, valitse ensin **Fault Tolerance** | **Break Mirror** ja sitten **Osio | Poista** (Partition | Delete). Vaikka peilauksen katkaiseminen ei poista tietoja, on kuitenkin suositeltavaa ottaa ensin varmuuskopiot tiedoista. Tämän jälkeen voit vapauttaa tilaa poistamalla jommankumman peilausparin osioista.

Jos toinen peilausparin osioista vahingoittuu vakavasti esimerkiksi virtakatkoksen tai ohjelmavirheen vuoksi, osiosta tulee **orpo** (*Orphan*). Tällöin sinun on ensin katkaistava peilaus (*Break Mirror*), jotta saat jäljelle jäävästä **toissijaisesta** osiosta erillisen levyn. Tällöin ehjänä säilynyt peilausparin osio saa **aseman kirjaimen**, joka oli aiemmin asetettu **koko peilausparille**.

Orpo osio saa seuraavan vapaana olevan aseman kirjaimen, mutta voit asettaa sille myös haluamasi kirjaimen. Tämän jälkeen voit luoda uuden peilausparin käyttämällä jonkin toisen levyn vapaata tilaa. Kun käynnistät mikron uudelleen, ehjän osion tiedot kopioituvat tähän peilausparin uuteen jäseneen.

Tapahtumien valvonta

Event Viewer on sovellus, jonka avulla valvotaan NT:n tapahtumia. Tapahtumat tallennetaan lokiin:

- **System Log** sisältää järjestelmän kirjaamat tapahtumat, esimerkiksi ohjaimen latausvirheet

- **Security Log** sisältää suojausjärjestelmän kirjaamat tapahtumat, esimerkiksi käyttäjän kirjautumisen järjestelmään. Oletuksena se ei ole käytössä, vaan se on sekä NT-työasemissa että -palvelimissa käynnistettävä erikseen **User Manager for Domains**issa **Policies** | **Audit**

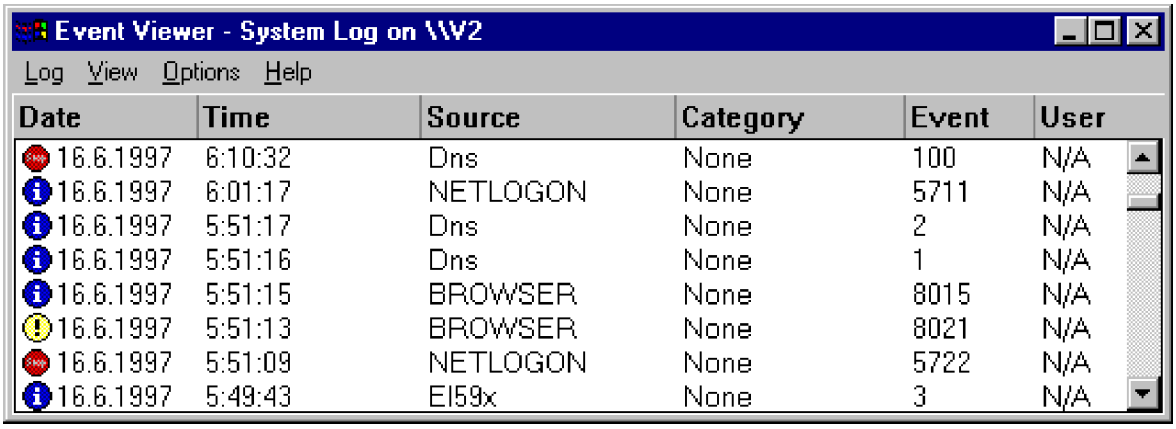
- **Application Log** sisältää sovellusten kirjaamat tapahtumat, esimerkiksi nauhavarmistusohjelman ilmoitukset.

Tapahtumien tyyppeihin kannattaa kiinnittää huomiota:

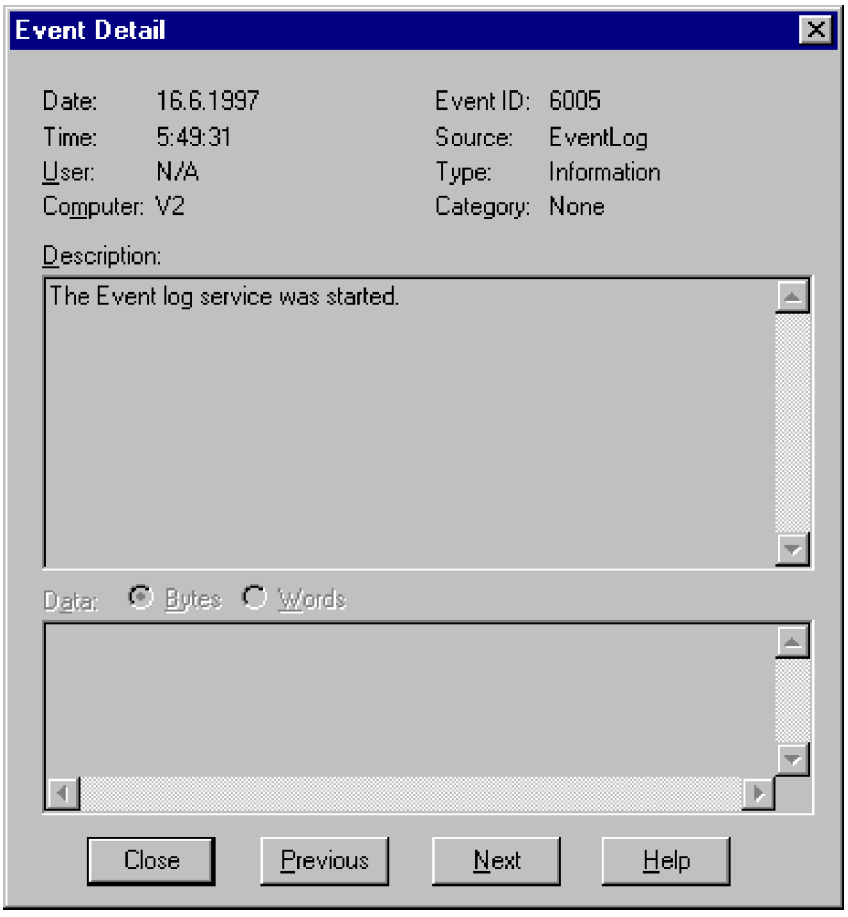
1) **Sininen** info-merkki on **ainoastaan tiedostusluontoinen** (Information), eikä viittaa esimerkiksi virhetilanteeseen. Toistuvat infotapahtumat viittaavat esimerkiksi palveluiden onnistuneeseen käynnistymiseen (esimerkiksi selauspalvelu, BROWSER)

2) **Keltainen** huutomerkki on **varoitus** (Warning), eikä viittaa *välttämättä* katastrofaaliseen ongelmaan, mutta saattaa kehittyä *jatkossa* ongelmaksi; esimerkiksi levytilan käyminen vähiin tuottaa varoituksen. Varoitukset on aina syytä tarkistaa!

3) **Punainen** stop-merkki on **virhe** (Error), **esimerkiksi palveluiden käynnistymisessä** tai **laiteohjainten lataamisessa** on tapahtunut virhetilanne. **Aiempi virhetilanne voi luoda uusia virhetilanteita!** Esimerkiksi verkkokortin laiteohjaimen latausongelma voi estää työasemapalvelun käynnistämisen. Siksi kannattaa seurata kaikki virhetilanteet, jotka ovat syntyneet esimerkiksi edellisen käynnistyskerran yhteydessä ja sen jälkeen ennen suuriluontoisia järjestelmän kokoonpanon muutoksia! Virheet on aina tarkistettava!



Koska **Event Log**-palvelu käynnistyy oletuksena automaattisesti, voit suodattaa näkyviin kaikki **eventlog**-palvelun käynnistymiset. Valitse ensin **System Log** ja suodata sitten esiin kaikki tapahtumat, joiden **lähde** (Source) on **eventlog**. Näin saat suodatetun listan, jossa ovat kaikki **eventlog-palvelun** käynnistykset, eli ajat, jolloin NT-kone on käynnistetty. Voit myös suodattaa esiin tapahtuman, jonka tunnus on **6005**.



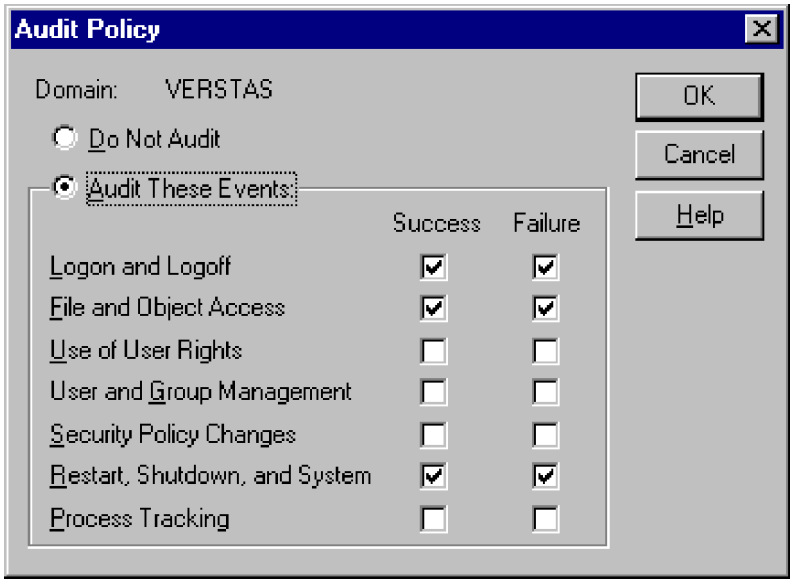
Jos epäilet NT-palvelimen käynnistyvän omia aikojaan, tarkista **Event log** -palvelun käynnistykset!

Suojauslokin käyttö järjestelmän valvonnassa

Määritä lokeihin tallennettavien **suojaustapahtumien** tyyppi valitsemalla **Policies** | **Audit**, millä määritetään lokiin merkittävät suojaustapahtumat.

Asetus on tehtävä tarvittaessa erikseen jokaisessa Windows NT -työasemassa; toimialueella **User Manager for Domains**issa annettu asetus koskee kaikkia toimialueen Windows NT -palvelimia - mutta ei Windows NT -työasemia!

Valitse halutut tapahtumat **Audit These Events** -listasta. Määritä tallennettavat tapahtumat valitsemalla haluamillesi tapahtumille onnistunut (**Success**) tai epäonnistunut (**Failure**)-toiminta tai poista niiden valinta.



Valittavat tapahtumat ovat seuraavat:

- **Logon and Logoff** - onnistuneet tai epäonnistuneet kirjausyritykset. Suojauslokin jokaisessa tapahtumassa on lisäksi selvitetty onko kyseessä **vuorovaikutteinen** (interactive), **verkon**

kautta suoritettu (network) vai **palvelun** (service) kirjausyritys.

- **File and Object Access** - onnistuneet ja epäonnistuneet suojattujen objektien käyttöyritykset (esimerkiksi kirjoittimet ja NTFS-levyn tiedostot).

- **Use of User Rights** - onnistuneet ja epäonnistuneet käyttöoikeuksien saantiyritykset sekä milloin ne on annettu. Pätee vain saantiaikaan, ei käyttöaikaan.

- **User and Group Management** on käyttäjätietokannan muutokset, kuten käyttäjän luominen ja ryhmäjäsenyyksien muuttaminen.

- **Security Policy Changes** on muutokset suojauskäytäntötietokantaan, kuten kirjauskäytäntöjen muuttaminen.

- **Restart, Shutdown, and System** on koko järjestelmän suojauksiin vaikuttavat toiminnot, kuten järjestelmän sammutus/käynnistys.

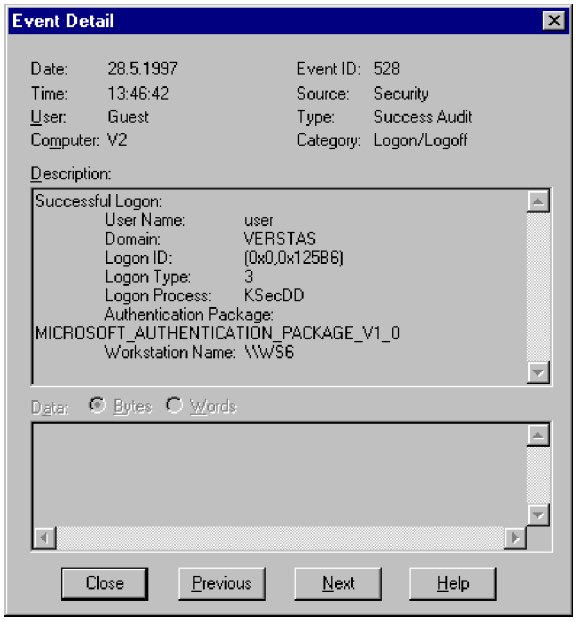
- **Process Tracking** - yksityiskohtaiset tiedot prosesseista.

Kun suojausloki on käytössä, **Security Log** sisältää suojausjärjestelmän kirjaamat tapahtumat, esimerkiksi käyttäjän kirjautumisen järjestelmään.

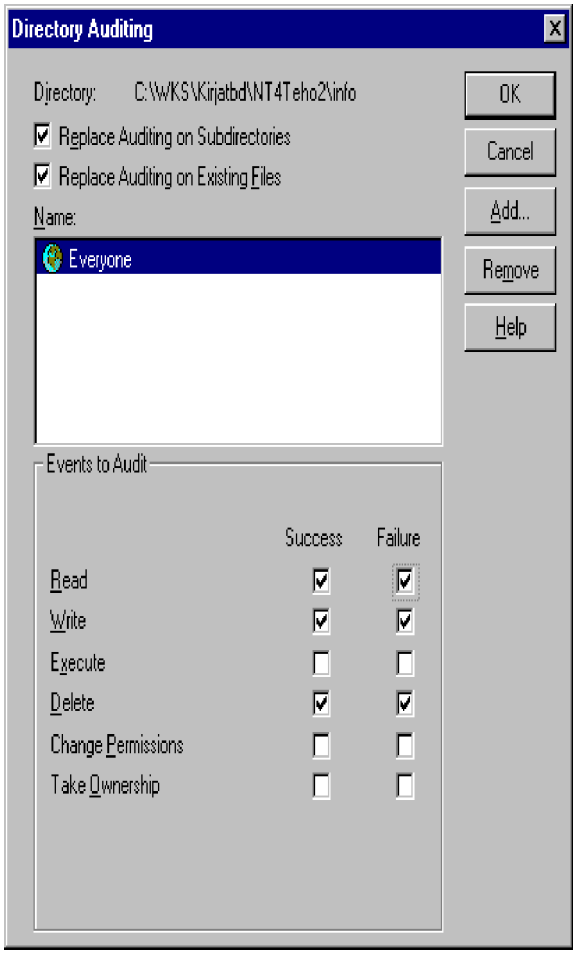
Suojauslokissa tyypit voivat olla **onnistuneita** tai **epäonnistuneita** valvontatoimintoja (Success Audit tai Failure Audit):

- **Success Audit** on onnistunut valvonta eli suojausten puitteissa onnistuneet toiminnot, esimerkiksi käyttäjä kirjautui järjestelmään onnistuneesti

- **Failure Audit** on epäonnistunut toiminta, esimerkiksi käyttäjän oikeudet eivät riittäneet resurssin käyttöön, esimerkiksi käyttäjän kirjautuminen järjestelmään ei onnistunut.



Kun **File and Object Access** on valittu käyttöön, NTFS-levyllä voidaan hakemiston tai tiedoston **Properties** | **Security** | **Auditing**-valinnalla valita objektien käyttöyritykset. Samoin voidaan kirjoittimia valvoa.



Suojauslokin asetuksiin **Log | Settings** on syytä kiinnittää huomiota. Asetukset ovat:

- **Change Settings** - valitse loki
- **Maximum Log Size** - koko on asetettava erikseen jokaiselle lokille!
- **Overwrite Events as Needed** - kun loki täyttyy, kirjoitetaan vanhimpien tapahtumien päälle
- **Overwrite Events Older than Days** - kirjoitetaan tietyn ikäisten tapahtumien päälle
- **Do Not Overwrite Events (Clear log Manually)** - lokia ei tyhjennetä mitenkään, vaan se on tyhjennettävä erikseen.

Luvussa **11** on käsitelty rekisterin asetusta **CrashOnAuditFail**, jolloin suojauslokin täyttyessä järjestelmä kaatuu automaattisesti. Asetuksella ei kuitenkaan ole merkitystä, jos on valittu käyttöön **Overwrite Events as Needed**, koska tällöin loki ei koskaan täyty.

LOGEVENT

Resource Kitin **LOGEVENT**-apuohjelmalla voi kirjoittaa tapahtumia lokiin.

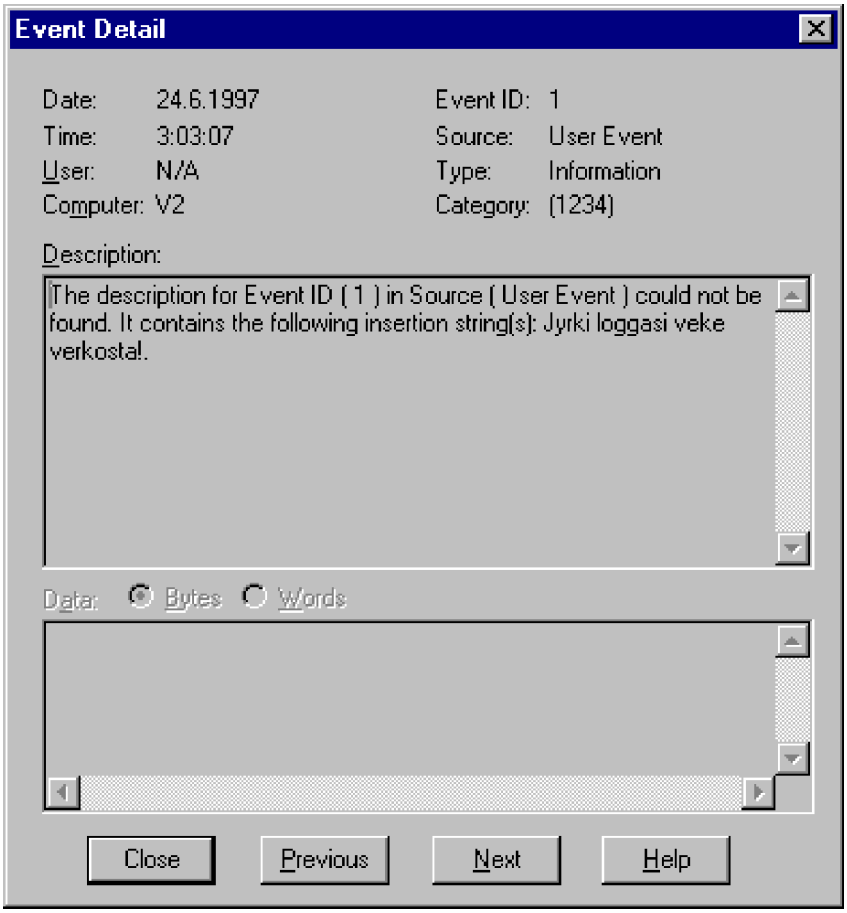
Syntaksi on:

logevent [-m \\kone] [-s SIWEF] [-c luokka] "Teksti"

-s (S)uccess, (I)nformation, (W)arning, (E)rror tai (F)ailure.

Esimerkiksi:

logevent -s S -c "Jyrki loggasi veke verkosta!"



Käytännön vinkkejä

Seuraavassa joitakin sekalaisia vinkkejä käytännön tilanteisiin.

The credentials supplied conflict with an existing set of credentials

Tämä ilmoitus tulee tyypillisesti tilanteessa, jossa on annettu komentorivin **NET USE**-komento. Syynä on se, että kohteeseen on jo istunto toisella käyttäjätunnuksella. Siirry tällöin C:-asemaan ja anna komento

NET USE * /D

AutoExNT

AutoExNT on Resource Kitin mukana tuleva palvelu, joka käynnistää komentojonon AUTOEXNT.BAT jokaisen NT:n käynnistyskerran yhteydessä - riippumatta siitä, onko kukaan kirjautunut käyttäjäksi.

Asennus tehdään seuraavasti:

1) Kopioi **AUTOEXNT.EXE** ja **SERVMESS.DLL** **%System-root%/System32** -hakemistoon

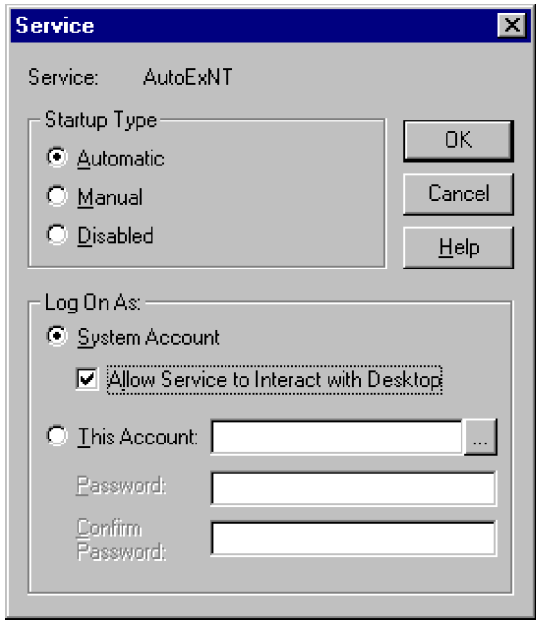
2) Tee **AUTOEXNT.BAT** -komentojono ja kopioi se **%System-root%/System32** -hakemistoon. Käytä komentojonossa hakupolkuja, koska käynnistysvaiheessa ei ole ympäristömuuttujia. Voit myös käynnistää palveluita **NET START**-komennoilla

3) Asenna palvelu komennolla **INSTEXNT install** tai **INSTEXNT install /interactive**, jolloin näet käynnistetyt komennot näytössä

4) Näyttöön tulee ilmoitus

CreateService AutoExNT SUCCESS
with InterActive Flag turned OFF

5) Määrittele lopuksi palvelu käynnistymään automaattisesti:



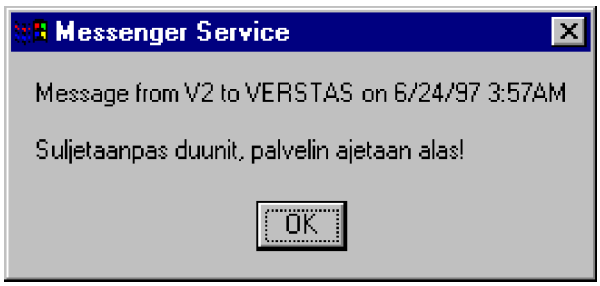
Käyttäjien avoimet tiedostot

Komennolla **NET FILE** tai **NET FILES** saadaan luettelo käyttäjien avoimista tiedostoista.

Ohjaamalla komento tiedostoon voidaan tutkia, onko käyttäjillä avoimia tiedostoja: seuraavassa on esimerkkinä itseään kutsuva **SHUT.CMD**, joka ajaa palvelimen alas vasta kun kaikki tiedostot on suljettu:

```
@echo off
NET FILES > C:\TEMP\F.TXT
findstr /B "There" C:\TEMP\F.TXT > NUL
if errorlevel 1 goto user
if errorlevel 0 goto alas
:alas
NET SEND /DOMAIN:VERSTAS Palvelin ajetaan alas!
sleep 30
SHUTDOWN /L
:user
NET SEND /DOMAIN:VERSTAS Suljetaanpas duunit, palvelin ajettaisiin alas!
sleep 30
SHUT.CMD
```

Järjestelmäkäytäntö lukinnut pääkäyttäjän



Ikävä tilanne, jossa järjestelmäkäytäntö (System Policy) on lukinnut pääkäyttäjän joko siten, että Policy Editorin tai rekisterieditorin käyttö ei ole mahdollista, on kierrettävissä ehkä jommalla kummalla seuraavista tavoista:

- Kirjaudu a.o. tunnuksella käyttäjäksi ja ota Policy Editorilla yhteys a.o. NT-koneeseen verkon kautta. Muuta **HKEY_CURRENT_USER**in asetuksia

- Toinen tapa (tilanteissa, joissa esimerkiksi **NTConfig.pol** on lukinnut kaiken mahdollisen) on joko kirjautua NT-työasemaan käyttäjäksi (ei toimialueelle) ja luoda/muuttaa pääkäyttäjän tunnus, joka on salasanoineen identtinen toimialueen pääkäyttäjätunnuksen kanssa. Kirjaudu tällä tunnuksella työasemaan ja yritä muuttaa Policy Editorilla **NTConfig.pol**-tiedostoa, uudelleennimeä se ja/tai muuta verkon yli NT-koneiden asetuksia.

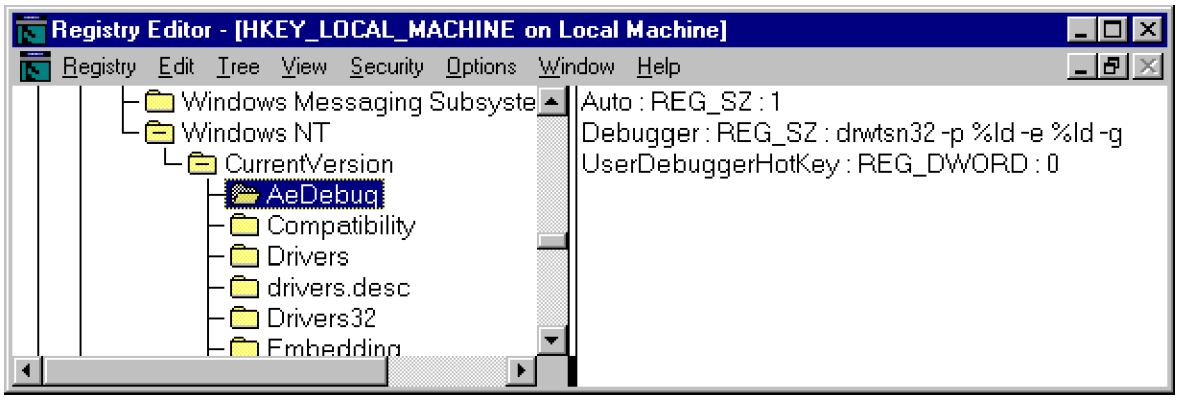
Sivutustiedoston poistaminen

Sivutustiedoston poistaminen automaattisesti järjestelmän sammutuksen yhteydessä tehdään rekisterissä asetuksella:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\SessionManager \MemoryManagement**
Nimi	**ClearPageFileAtShutdown**
Tyyppi	**REG_DWORD**
Arvo	**0 - ei poisteta (oletus), 1 - poistetaan**

Dr Watsonin deaktivointi

Rekisterissä on useita asetuksia Dr Watsonista.



Dr Watsonin poistaminen käytöstä tehdään rekisterissä asetuksella:

Polku	**HKEY_LOCAL_MACHINE\SOFTWARE**
Avain	**\Microsoft\WindowsNT\CurrentVersion\AeDebug**
Nimi	**Auto**
Tyyppi	**REG_SZ**
Arvo	**0 - ei käytössä, 1 - käytössä (oletus)**

Voit myös ottaa käyttöön jonkin toisen debuggerin antamalla sen käynnistyskomennon **Debugger**-kohtaan.

Viestit

Reaaliaikaista viestinlähetystä voi käyttää monella tavalla. Esimerkiksi kirjauskomentojonoon voi lisätä käyttäjän tutkimisen:

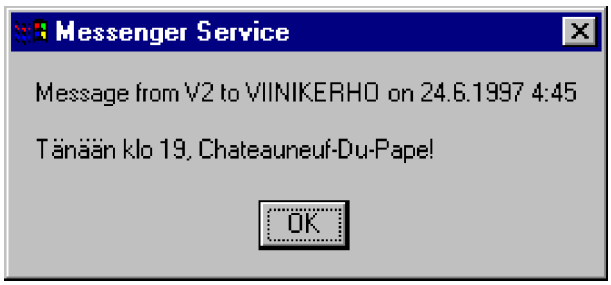
if %username%x==PerttiMx NET NAME VIINIKERHO /ADD

Tässä tapauksessa jos käyttäjätunnus on **PerttiM** (x tutkii syntaksin), käyttäjän työasemaan lisätään nimi **VIINIKERHO**.

Komennolla

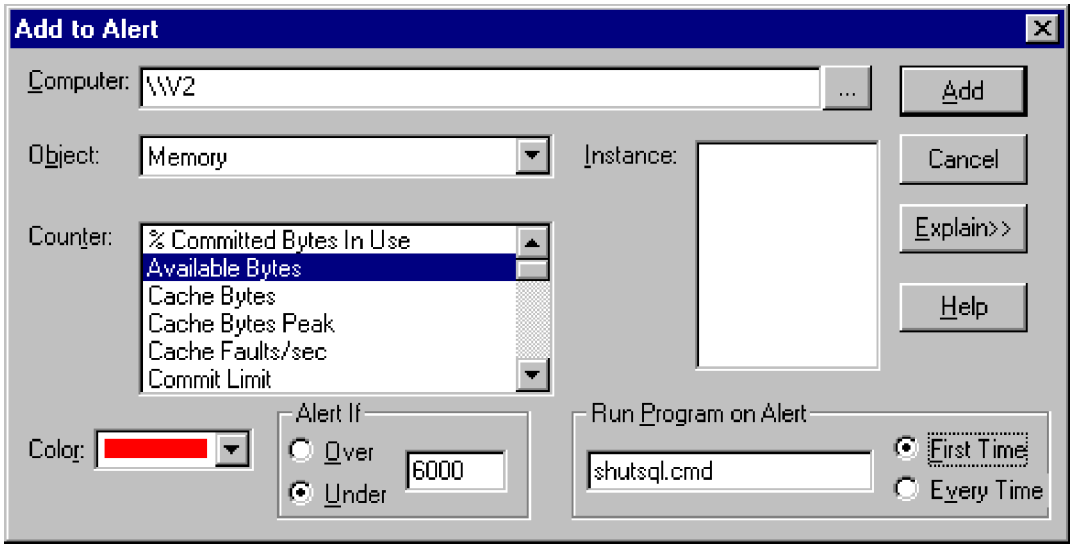
net send VIINIKERHO Tänään klo 19, Chateauneuf-Du-Pape!

Saadaan kaikille käyttäjille, joiden työasemassa on nimi **VIINIKERHO**, ilmoitus:

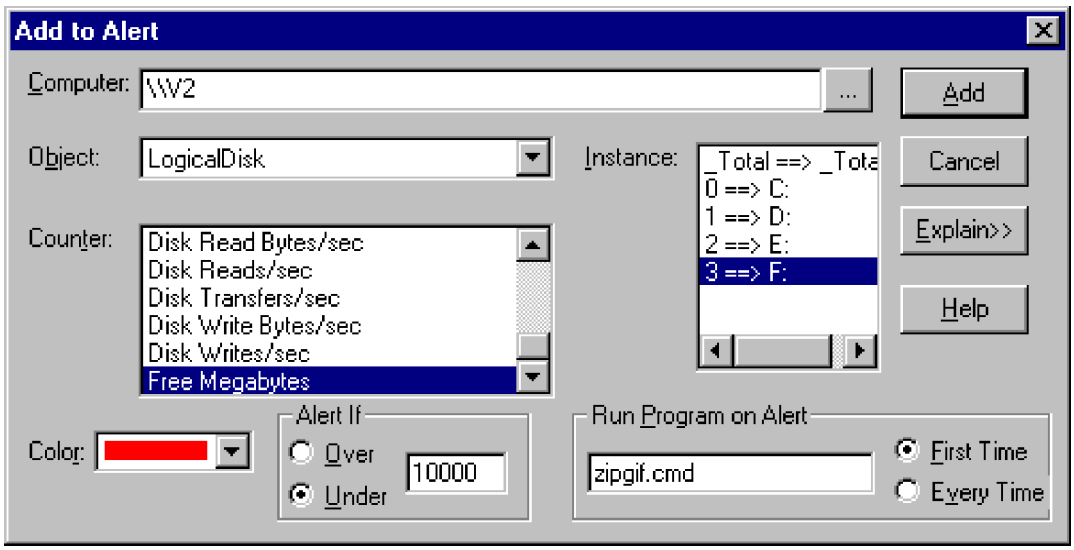


Hälytykset

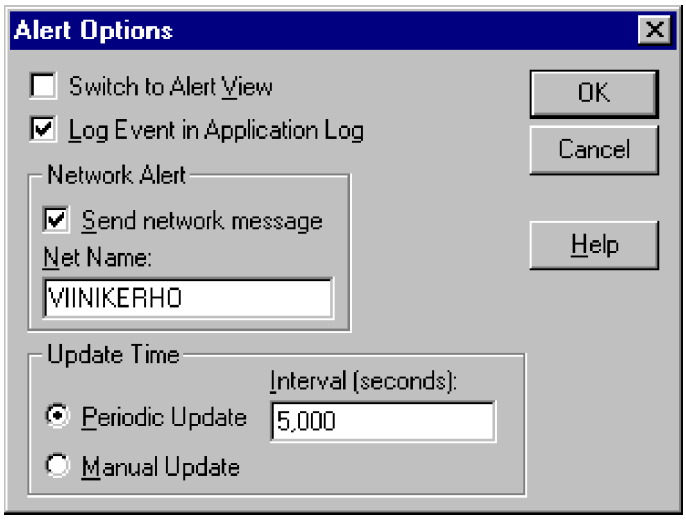
Voit käyttää **Performance Monitorin** hälytys (Alerts)-ominaisuuksia hyväksesi monellakin tavalla. Tässä esimerkissä palvelimen vapaan muistin pudotessa alle 6000 tavua ajetaan komentojono **SHUTSQL.CMD**, joka sammuttaa SQL Serverin kyseisessä palvelimessa, mikä vapauttaa samalla muistia. - Voi olettaa, että esimerkissä SQL Server ei ole palvelimen kriittisin palvelu.



Tässä esimerkissä palvelimen vapaan levytilan pudotessa F:-asemassa alle 10000 tavua ajetaan komentojono **zipgif.cdm**, joka esimerkiksi pakkaa levyasemassa olevat GIF-tiedostot. Tällöin saadaan lisää levytilaa käyttöön.



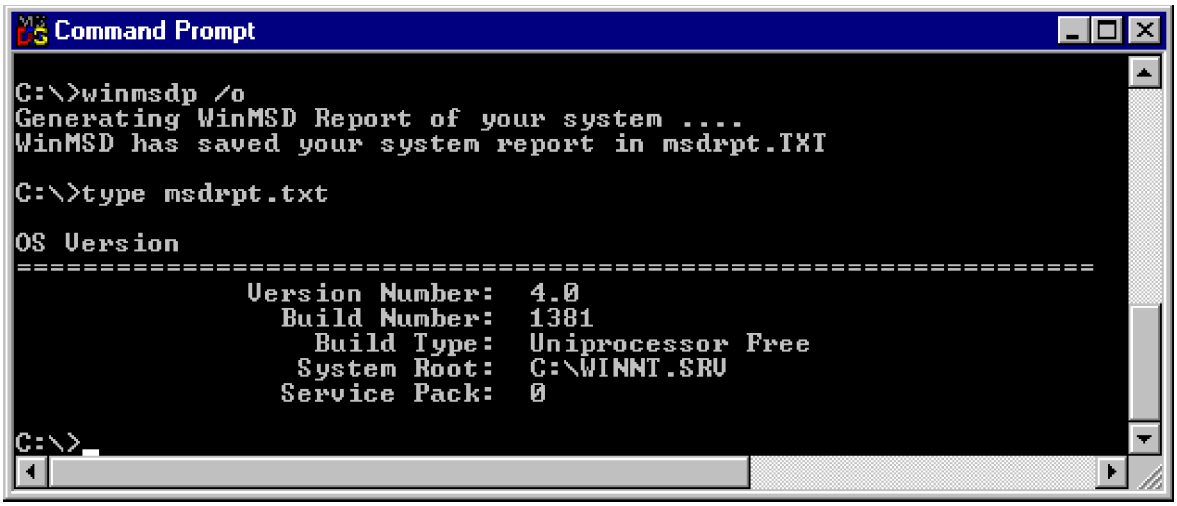
Komentojonoissakin voi käyttää **NET SEND**-komentoja, mutta **Options | Alert**-valinnalla voit ohjata viestit rekisteröidylle nimelle. Kohde voi olla myös työasema - \\-merkkejä ei tarvita.



Voit myös ketjuttaa hälytyksiä siten, että käynnistät komentoriviltä uuden Performance Monitorin seuraamaan uutta asiaa esimerkiksi komennolla **PERFMON DUKE.PMA DOOM.PMA**.

WinMSDP

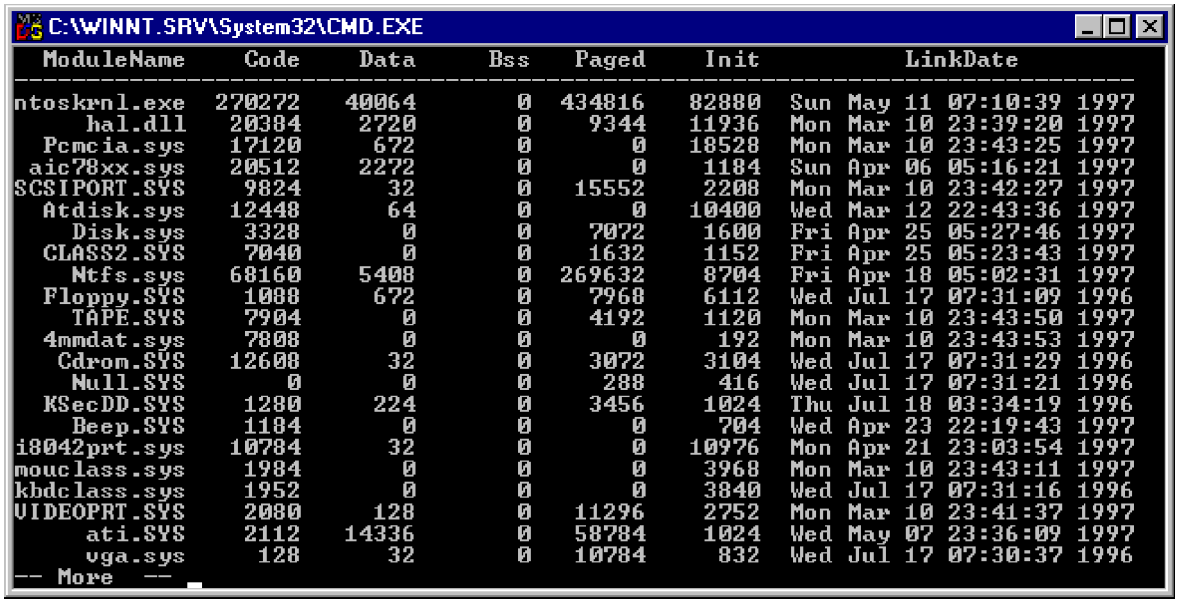
WINMSDP on Resource Kitin apuohjelma, joka tulostaa tiedostoon laitteiston asetukset.



Ohjelma tuntee useita valitsimia, esimerkiksi **/O** tulostaa käyttöjärjestelmän asetukset.

Drivers

DRIVERS on Resource Kitin apuohjelma, joka näyttää laiteohjainten tiedot.



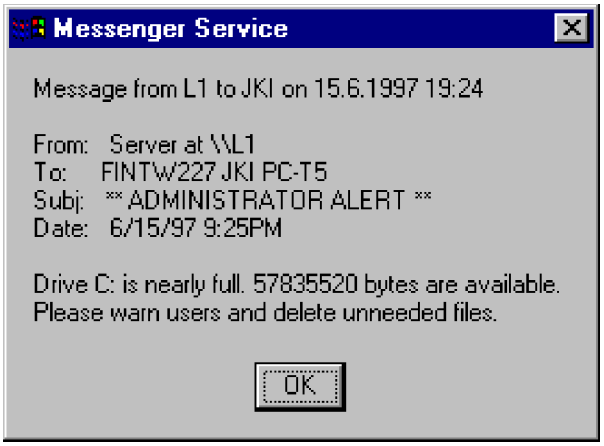
Voit lisätä esimerkiksi komennon

DRIVERS > \\V1\DATA\%COMPUTERNAME%.DRIVERS.TXT

kirjauskomentojonoon, niin saat kerättyä automaattisesti NT-koneen nimiset tiedostot laiteohjaimista.

Levytilan ilmoitus

Oletuksena saat ilmoituksen, kun vapaata levytilaa on jäljellä 10%.



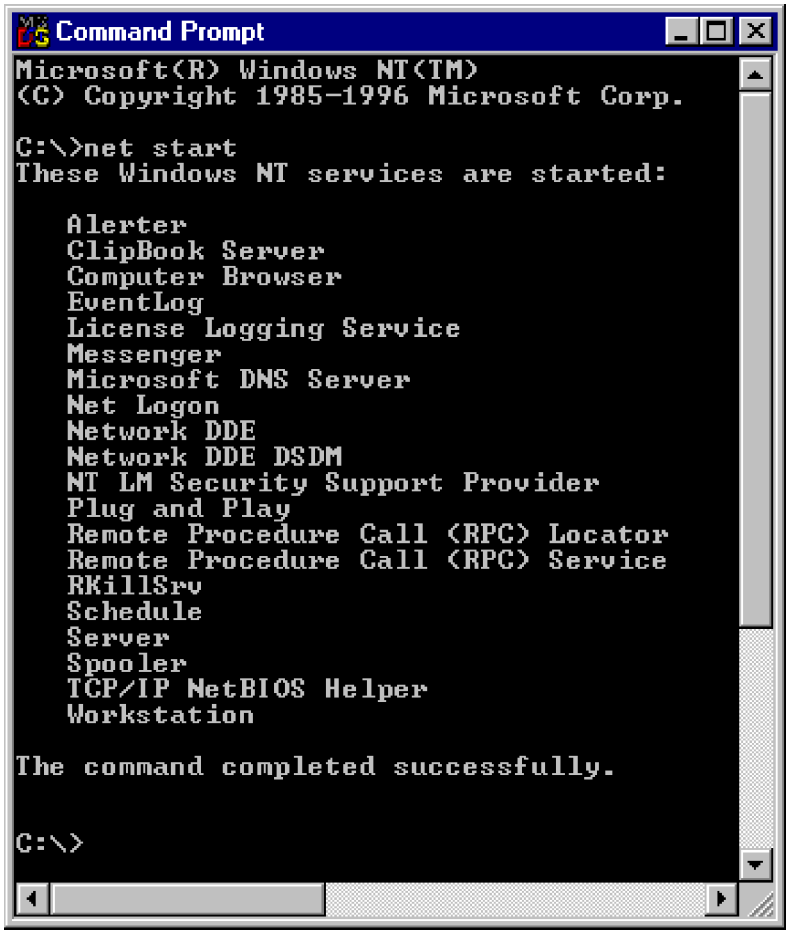
Voit muuttaa asetusta rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Services\LanmanServer\Parameters**
Nimi	**DiskSpaceThreshold**
Tyyppi	**REG_DWORD**
Arvo	**0 - 99 prosenttia, 10 oletus**

Anna haluttu koko prosentteina.

Palvelimen alasajo

Palvelimen hallitun alasajon voi toteuttaa myös komentojonolla:



1) Anna komento **NET START > tiedosto**

2) Muokkaa tiedostoon tallennettuja rivejä siten, että jokaisen rivin alussa lukee **NET STOP** ennen a.o. palvelua ja palvelu on tarvittaessa lainausmerkeissä, esimerkiksi
NET STOP Plug and Play

3) Älä muuta rivien järjestystä! Tallenna muokattu tiedosto vaikkapa nimellä **SHUT.CMD**. Komentojono ajaa palvelimen hallitusti alas.

NTFSDOS

NTFSDOS-apuohjelmalla voidaan tehdä käynnistyslevyke, jolla päästään käsiksi NTFS-tiedostojärjestelmällä suojattuihin hakemistoihin ja tiedostoihin.

Sen käyttö edellyttää pääsyä palvelimen levykeasemaan ja palvelimen uudelleenkäynnistystä, eli tässä on jälleen yksi syy lisää suojata palvelin myös fyysisesti!

Pääkäyttäjät ja tukihenkilötkin voivat tarvittaessa käyttää tätä menetelmää hyväkseen päästäkseen käsiksi vaurioituneeseen tai liiankin hyvin suojattuun NT-koneeseen.

Katso **http://www.ntinternals.com/ntutil.htm**.

NTFS-buuttidisketti

Jos NT-asennus toimii todennäköisesti muuten, mutta käynnistystiedostoissa on jotain sekaisin, voit kokeilla NTFS-buuttidiskettiä. Se tehdään seuraavasti:

1) Tee kopio **Setup Disk 1**:stä

2) Poista kaikki tiedostot kopiolta

3) Kopioi **NTDETECT.COM** ja **NTLDR** levykkeelle

4) Uudelleennimeä **NTLDR** nimelle **SETUPLDR.BIN**

5) Tee levykkeelle NT-konetta vastaava **BOOT.INI**. Esimerkiksi NT-koneessa jossa on yksi SCSI-levyosio käynnistyslevyllä:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT.SRV="NT4Srv" /basevideo /sos
```

6) Anna levykkeen tiedostoille tiedostomääreet System, Hidden, Read-Only:

ATTRIB NT*.* +R + S +H
ATTRIB BO*.* +R + S +H

7) Käynnistä NT-kone levykkeellä. Onnea!

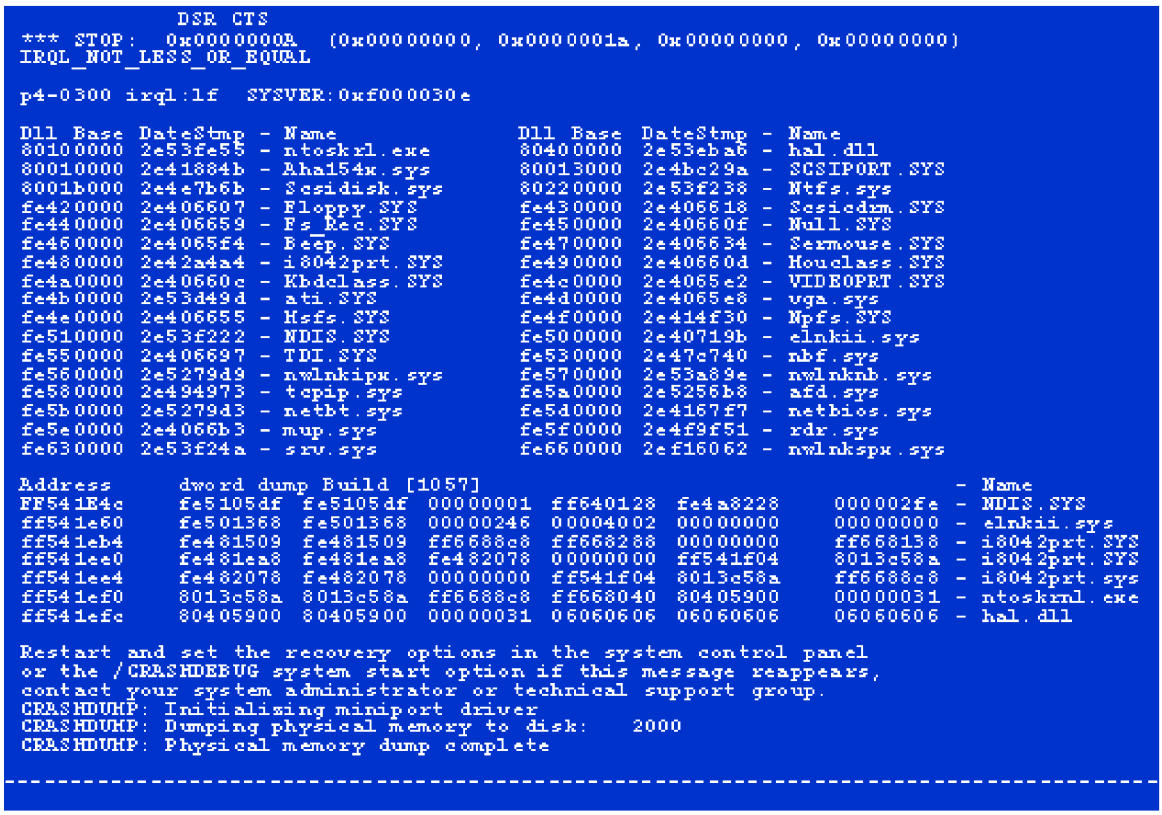
Käynnistysongelmat

NT-palvelimen käynnistyksessä voit saada seuraavia ilmoituksia - taulukossa on kuvaus toimenpiteistä:

Puuttuva tiedosto	Virheilmoitus	Kuvaus
NTLDR	BOOT: Couldn't find NTLDR. Please insert another disk.	NTLDR on palautettava CD-ROM:ilta
NTDETECT.COM	Fatal System Error: 0x00000067 - Configuration Initialization Failed	Tarkista BOOT.INI; NTDETECT.COM on ehkä palautettava CD-ROM:ilta
BOOTSECT.DOS	Couldn't open boot sector file multi(0)disk(0)rdisk(0)partition(1):\bootsect.dos	Multiboot-järjestelmässä; voit kopioida täsmälleen samanlaisesta järjestelmästä (hakemistorakenne, levy, osiot) BOOTSECT.DOS-tiedoston. Muuten joudut todennäköisesti asentamaan NT:n uudelleen.

Blue Screen of Death

Käynnistysvaiheen BSOD on varsin ikävä tilanne.



Ne ovat ytimen virhetilanteita, joista yleisimpiä on kuvattu seuraavassa taulukossa:

Virheilmoitus	Kuvaus
F002	Tavallisesti muistiin liittyvä, esimerkiksi erilaiset muistipiirit tai huonosti kiinnitetty muistipiiri
0000001E	Tavallisesti tiedostojärjestelmän ongelma; katso onko listalla viimeisimpinä RDR.SYS (ehkä verkkokortin virhe) tai NTFS.SYS tai FASTFAT.SYS (ehkä CHKDSK /F auttaisi asiaan)
0000000A	Keskeytyksen (IRQ), I/O-portin tai DMA-kanavan konflikti
0x0000007B	Järjestelmälevyn ongelma

0x00000069 tai 0x00000067	Kiintolevyohjainongelma; pudota DMA-kanavan nopeutta, tarkista SCSI-terminointi, laitekonfliktit, laiteohjain ja että NTDETECT.COM on käynnistyslevyn juurihakemistossa eikä järjestelmätiedostoja puutu
NMI Hardware Error	Laitteistovika; viallinen muisti, nopeuseroja muun laitteiston ja muistipiirien välillä jne. Tarkista muistipiirien kiinnitykset
IRQL_NOT_LESS_OR_EQUAL	Prosessi yritti päästä sivuttavaan muistiin käsiksi sisäisellä keskeytyksellä (IRQL), jonka prioriteetti on korkeampi kuin prosessin; se ei ole sallittua. Syynä voi olla huonosti toimiva laiteohjain

Mainittakoon vielä, että on myös olemassa mainio Blue Screen-näytönsäästäjä! Katso **http://www.ntinternals.com/ntutil.htm**.

Windows NT 4.0 Server Resource Kit

Seuraavat tässä kirjassa viitatut ohjelmat tulevat **vain** Windows NT Server 4.0 Resource Kitin mukana, eivät Windows NT 4.0 Workstation Resource Kitin:

- BREAKFTM.EXE - peilauksen palautus
- BROWMON.EXE -Browser-monitori
- BROWSTAT.EXE -Browser Status
- Crystal Reports Event Log Viewer
- dbWeb
- DHCPCMD.EXE -DHCP-hallinta
- DHCPLOC.EXE -DHCP Server-paikannus
- DOMMON.EXE -Domain -monitori
- EMWAC Server CGI Gateway -scriptit
- FINDGRP.EXE
- GETSID.EXE
- GRPCPY.EXE
- Index Server
- KIX32.EXE: KiXtart 95
- Mail Server
- NETSVC.EXE - palveluiden hallinta komentoriviltä

- RASLIST.EXE
- RASUSERS.EXE
- RCMD.EXE -etäkomennot (Remote Command Service)
- Remote Console
- RSHSVC.EXE -TCP/IP Remote Shell
- SNMPMON.EXE -SNMP-monitori
- SRVINFO.EXE
- TIMESERV.EXE -aikasynkronointi
- USRSTAT.EXE
- Web-hallintaohjelma Windows NT Serverille
- WINSCL.EXE
- WINSDMP.EXE.

Muita työkaluja

NT:n suosion kasvaessa apuohjelmia on tullut huomattavasti tarjolle. Joitakin esimerkkejä:

- **NetOff**, järjestelmän sulkeminen, **http://www.citadel.com**
- **BindView**, analysointiohjelma, **http://www.bindview.com**
- **Cinco NetXRay**, protokolla-analysaattori, **http://www.cinco.com**
- **DKHelp Desk**, Help Desk, **http://www.dksystems.com**
- **DeliverIT!**, ohjelmistojen jakelu, **http://www.gsnetworks.com**
- **NobleNet Web**, ohjelmistojen jakelu, **http://noblenet.com**
- **Unison Maetro**, ajoitussovellus, **http://www.unison.com**
- **Standby Server**, vikasietoisuuspalvelu, **http://www.vinca.com**
- **NetAttaché**, WWW-tietojen päivitys, **http://www.tympani.com**
- Levynhallintaohjelmia ym, **http://www.ntsoftdist.com**.

Myös varsinaisia hallintatyökalujakin on tullut tarjolle. Seuraavassa pari kirjoittajan suosikkia:

- **Admin!NT** on mahdollistaa NT-ympäristön palveluiden ja käyttäjien hallinnan keskitetysti yhdellä työkalulla. Lisätietoja: **http://www.netwinsoft.com**

- **NetManage** on tarkoitettu enemmän verkon TCP/IP-asetusten ja -palveluiden hallintaan. Myös se tarjoaa yhdestä sovelluksesta palveluiden hallinnan keskitetysti. Lisätietoja: **http://www.netmanage.com**.

Optimointi

Verkko on tarkoitettu yhdistämään siihen liitetyt työasemat muihin laitteisiin kuten kirjoittimiin, tietoliikennelaitteisiin ja massamuisteihin siten, että näiden jaettujen resurssien **käytettävyys** on mahdollisimman hyvä. Alkuperäinen ajatus verkottamisesta perustui siihen, että näin kalliita laitteita voidaan käyttää mahdollisimman **kustannustehokkaasti** (*Cost-Efficiency*). Näin henkilökohtaiset tietokoneet (*Personal Computer*, PC) muuttuivat verkon osasiksi, työasemiksi, ja samalla käyttäjät voivat jakaa informaatiota keskenään. Suuntaus on edennyt siten, että käyttäjät voivat jopa yhdessä muokata olemassaolevaa ja tuottaa uutta informaatiota työryhmäohjelmistojen (*Workgroup Computing*) avulla. Internet-teknologiat ovat tuoneet tullessaan avoimet standardit ja rajapinnat. Tällöin toimivasta verkosta palveluineen on tullut toiminnan **edellytys**, ei pelkästään **apuväline**.

Kaikista verkon tietokoneista tärkeipiä ovat palvelimet, ja niillä on suuri vaikutus koko järjestelmän suorituskykyyn. Palvelimiin on asennettu Windows NT Server-verkkokäyttöjärjestelmä ja verkkosovellukset sekä niiden datatiedostot, ja niiden varaan on suunniteltu koko järjestelmän vikasietoisuus- ja virheenkorjausominaisuudet sekä tietoturva.

Järjestelmän **optimoinnin** tavoite on määrittää, mikä laitteistoresurssi kohtaa suurinta kysyntää muodostaen **pullonkaulan** (*Bottleneck*) ja säätää toimintaa siten, että tuo kyseinen vähenee ja tehokkuus paranee.

Järjestelmän pitäisi rakentua siten, että sen resursseja käytetään tehokkaasti ja resurssit jaetaan tasapuolisesti käyttäjien kesken. Tämä ei ole ollenkaan niin vaikeaa, jos noudatetaan muutamaa sääntöä ja ymmärretään järjestelmän perustoiminta:

- **Tiedosto- ja tulostuspalvelinympäristössä** suurin osa palvelimen toiminnoista tukee tiedosto- ja tulostuspalveluja. Levyä käytetään usein paljon, koska useita tiedostoja avataan ja suljetaan. Myös verkkokorttien kuormitus on raskasta, koska tietoa

siirretään suuria määriä. Muisti ei tavallisesti saa osakseen suurta kuormitusta tällaisessa ympäristössä, vaikka muistia voidaankin käyttää paljon, koska tiedostojärjestelmän välimuistille voidaan varata paljon muistia. Tällaisessa ympäristössä myös prosessorin käyttö on tyypillisesti vähäistä

- **Sovelluspalvelinympäristö** taas (esimerkiksi Microsoft BackOffice -tuotteet Microsoft SQL Server, Microsoft Systems Management Server ja Microsoft SNA Server) vaatii huomattavasti enemmän prosessoritehoa ja keskusmuistia kuin tyypillinen tiedosto- ja tulostuspalvelinympäristö, koska itse palvelimella tapahtuu paljon enemmän varsinaista tietojenkäsittelyä.

Varmin tapa saada jokin käsitys järjestelmän käytöstä on **seurata** niitä, ja yksi tehokkaimmista välineistä siihen on Windows NT:n **Performance Monitor**. Jokaisella NT-koneella voidaan valvoa eri **objektien** (*Objects*) tehokkuutta, esimerkiksi prosessoreita, muistia, välimuistia, säikeitä ja prosesseja. Jokaiseen näistä liittyy **laskureita** (*Counters*), jotka antavat tietoja esimerkiksi laitteen käytöstä, jonojen pituuksista ja viiveistä sekä tietoja, joiden avulla voidaan mitata suorituskykyä ja ruuhkautumista. Performance Monitorissa on kartoitus-, hälytys- ja raportointiominaisuudet, jotka näyttävät tilanteen ja pitävät jatkuvasti lokia. Lokitiedostoja voidaan selailla ja tutkia myös myöhemmin.

Ennen kuin ostat lisää laitteita tai laitteiston päivityksiä, kannattaa seurata ja säätää järjestelmää Performance Managerin avulla ja ottaa olemassa olevat resurssit mahdollisimman tehokkaaseen käyttöön.

Esimerkiksi:

- Jos huomataan, että prosessorin käyttöaste on 100%, kannattaa ennen nopeamman tai lisäsuorittimen hankkimista tunnistaa ja analysoida **prosessia**, joka kuluttaa eniten prosessoriaikaa. Prosessoriaikaa saattaa kulua kiintolevyn ohjaimeen, joka käyttää ohjelmoitavaa I/O:ta (*Programmed IO*, PIO). Tässä tapauksessa DMA-levyohjain vähentää suoritintehon kulutusta.

- Jos huomataan, että kiintolevy on täynnä, ei kannata hankkia uusia levyasemia ennen kuin on todettu, kuinka suuri osa sivutustiedostosta on käytössä. Järjestelmän sivutustiedosto (*Paging file*) on ehkä alustettu 200 Mt:lle, mutta siitä on käytössä enimmillään 40 Mt. Uuden kiintolevyn ostamisen sijaan voidaan ainakin väliaikaisena ratkaisuna säätää sivutustiedoston

kokoa.

Seuraavaksi käsitellään palvelinlaitteiston valintaan ja Windows NT-palvelimen optimointiin liittyviä kysymyksiä. Näkemykset edustavat kirjoittajan subjektiivista mielipidettä.

Palvelinlaitteisto

Windows NT-palvelinlaitteiston kokoonpanoon vaikuttavat eri kriteerit kuin tyypillisen työaseman.

Palvelimen tulee olla nopea, luotettava, laajennettava ja turvallinen. **Tiedostopalvelimen** (*File Server*) ollessa kyseessä on hyvä muistaa, että se saattaa usein olla yrityksen tärkeimpien tietojen talletuspaikka, ainakin jos siellä sijaitsee niin käyttäjien kotihakemistot, sähköpostin palvelut kuin sovelluksetkin, jotka käyttäjät lataavat omiin työsemiinsa.

Eräs luokittelu on **työryhmä**- (*Workgroup*) ja **osastotason** (*Departmental*) palvelimet. Tällöin tarkoitetaan käyttäjämäärien jakautumista siten, että työryhmätason palvelin pystyy tarjoamaan palveluita 12 - 60 käyttäjälle, osastotason palvelin taas 60 - 200 käyttäjälle. Tämä erottelu näkyy myös hinnassa. Tyypillisesti osastotason palvelin tarjoaa paremman laajennettavuuden, suorituskyvyn ja vikasietoisuuden.

Jos haluat ostaa sekä halvan että laajennettavan/suorituskykyisen palvelimen, joudut ostamaan molemmat.

Työasemamikro *ei* ole palvelinmikro.

Palvelimen tehokas käyttöikä on tyypillisesti kaksi - kolme vuotta. Tämän jälkeen päivitys alkaa maksaa enemmän (tai on ainakin kyseenalaista) verrattuna uuden, tehokkaamman palvelimen hankintaan.

Käyttötarkoitus

Palvelimen käyttötarkoitus on keskeinen tekijä (tai ainakin sen tulisi olla) määriteltäessä laitteiston kokoonpanoa. Esimerkiksi **tiedostopalvelimien** pullonkaulaksi ei yleensä muodostu prosessorin nopeus - niinpä mikä tahansa **Pentium**-tason (133 MHz tai enemmän) laite tyypillisesti käy mainiosti tähän tehtävään. Keskusmuistin määrä ei myöskään **tiedosto-**

palvelimien kohdalla ole merkittävä, mutta etäkäyttöpalvelimissa (*Remote Access Server*) sen sijaan on. Myös **tietokantapalvelimet** (*Database Server*) ja **Internet-palvelimet** (esimerkiksi *Internet Information Server*) vaativat palvelimelta vääntöä - sekä keskusmuistia että prosessorin suorituskykyä. Seuraavat ehdotukset palvelinten minimikokoonpanoista perustuvat kirjoittajan subjektiivisiin näkemyksiin:

- **Tiedostopalvelin**: **32 - 64 Mt RAM**, **Pentium 133 MHz** tai nopeampi, vikasietoinen **nopea levyjärjestelmä** (RAID 1 tai RAID 5) ja **nopea verkkokortti**

- **Etäkäyttöpalvelin** - **64 Mt tai enemmän RAM**, **Pentium 100 MHz** tai nopeampi

- **Sovelluspalvelin** (*Application Server*)**, Tietokantapalvelin** tai **IIS-palvelin** - **64 Mt tai enemmän RAM**, **Pentium Pro 150 MHz** tai nopeampi (tai useampia), vikasietoinen **nopea levyjärjestelmä** (RAID 1 tai RAID 5) ja **nopea verkkokortti**. Moniprosessoripalvelimissa aloituskokoonpano voi toki olla pienempi, ja prosessorien lukumäärää voidaan kasvattaa suorituskyvyn tarpeen kasvaessa. Sovelluspalvelimella tarkoitan esimerkiksi **Lotus Notes**-palvelinta, en tiedostojen jakamiseen perustuvaa palvelinta (esimerkiksi MS Office - ks. Tiedostopalvelin)

- **Sähköpostipalvelin** (*E-mail Server*) - riippuu sähköpostipalvelimen toteutustavasta - joko kyseeseen tulee tiedostopalvelintyyppinen ratkaisu (*MS Mail*) tai sovelluspalvelintyyppinen ratkaisu (*MS Exchange*).

- **Ohjauskoneiden** (*Domain Controller*) kohdalla kannattaa lisäksi muistaa käyttäjätietokannan koon asettamat vaatimukset (ks. Luku 5).

Merkkivalmistajan laite vai itse rakennettu

Mielenkiintoinen kysymys on, tulisiko palvelimen olla ns. merkkivalmistajan (Compaq, Hewlett-Packard, ICL, IBM, AST, NCR, Tandem, Digital, Dell jne) laite vaiko kävisikö itse rakennettu. Erityisesti palvelinkäyttöön tarkoitettuja mikroja on ollut saatavilla lähes 10 vuotta (ensimmäisenä valmistajana Compaq SystemPro-palvelimellaan).

Kirjoittajan mielipide on, että *jos* tarvitaan esimerkiksi tehokasta levyjärjestelmää ja todennäköisesti hyvin yhteensovitettuja komponentteja, merkkivalmistajan laite on paremmin suunniteltu kuin mihin omassa ympäristössä tavanomaisilla välineillä kyetään.

Tällä en tarkoita etteikö esimerkiksi Intelin emolevyllä, Adaptecin SCSI-ohjaimella ja 3Comin verkkokortilla toteutettu mikro toimisi palvelimena siinä kuin merkkivalmistajan laitekin. Ongelmaksi saattaa muodostua oma osaaminen (tai sen puute), takuisiin liittyvät kysymykset sekä kuka *muu* pystyy huoltamaan tai ylläpitämään laitteiston. Laitteistoon sinällään liittyy myös virtalähteen mitoitus ja toimintavarmuus sekä kotelon sisäinen tuuletus.

Kirjoittaja on käyttänyt itserakennettuja palvelimia menestyksellisesti useita vuosia esimerkiksi tulostuspalvelimina. Kokemuksen perusteella kirjoitajan subjektiivinen näkemys on seuraava:

- Itserakennettu palvelin on todennäköisesti erittäin toimiva ns. standardikomponenteilla (Intel, Adaptec, Matrox, 3Com jne)

- Vikasietoisuus ei todennäköisesti ole samaa luokkaa kuin merkkivalmistajien laitteilla - tämä näkyy ehkä edullisemmassa hinnassa. Kannattaa vertailla, mitä halvimmat vastaavalla kokoonpanolla varustellut merkkipalvelimet maksavat. Jos itserakennetussa palvelimessa ei ole vikasietoista levyjärjestelmää (RAID), nauhavarmistuslaite on pakollinen!

- Itserakennetun palvelimen laajentaminen saattaa olla edullisempaa ja helpompaa (johtuen standardikomponenteista) kuin merkkipalvelimen. Ongelmat joutuu myös itse selvittämään. Muista varalaitteiston merkitys!

- Yritysmaailmassa itserakennettujen palvelinten hankinta saattaa olla huonosti perusteltavissa. Sen sijaan esimerkiksi koulu- ja oppilaitosympäristöissä halvempi palvelin saattaa olla perusteltavissa hintaerolla, säästöillä tms

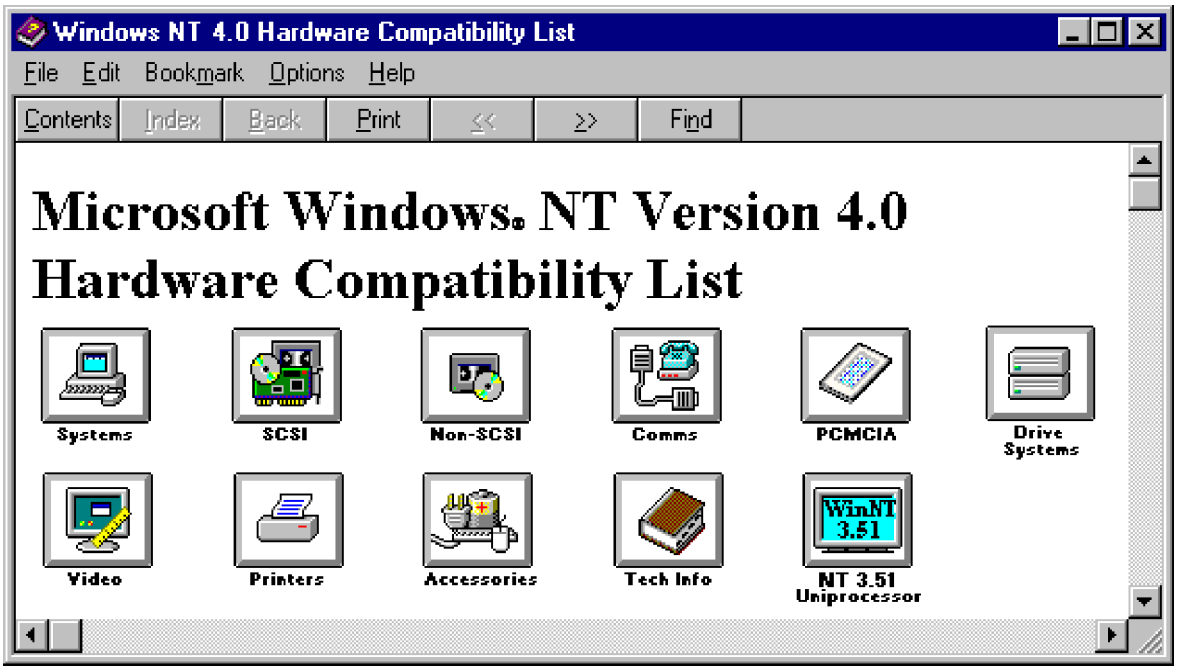
- Käyttötarkoituksiin, joissa palvelin on väliaikaisesti tai pysyvästi korvattavissa varajärjestelyillä tai varapalvelimilla itserakennettu palvelin saattaa soveltua. Jos palvelin on kriittisessä käytössä - esimerkiksi sähköpostipalvelimena tai sovelluspalvelimena - kannattaa harkita merkkipalvelimen hankintaa

- Merkkipalvelimen sisäänrakennettu SCSI-ohjain ja verkkokortti ei välttämättä edusta tehokkainta mahdollista - vaan halvinta mahdollista, jolla voidaan tällaisenkin liitännän olemassaolo mainita

- Muista, mikä ero on **järkevällä** ja **mielenkiintoisella hankinnalla**. Ero tulee tyypillisesti selville ensimmäisessä vikatilanteessa. Hanki kriittiseen käyttöön merkkivalmistajan ratkaisu ja keskity mielenkiintoisiin ratkaisuihin, *jos* aikaa riittää.

Edelläolevalla luettelolla **en** tarkoita, että kaikkien laitevalmistajien kaikki palvelinratkaisut olisivat loistavia saati edes toimivia. Todennäköisyys siihen, että voit työntää ongelmat jonkun muun ratkottavaksi ovat kuitenkin suurempia.

Tarkista kaikissa tapauksissa laitteiston yhteensopivuus **Windows NT Hardware Compatibility List**-luettelosta. Uusimman löydät Intertistä osoitteesta **http://www.microsoft.com**. Tyypillisesti nimi on päiväyksen mukainen, esimerkiksi **HCLFEB97.HLP**.



Voit myös tutkia laitteiston asetukset **Windows NT Hardware Query Tool**illa ja **SCSI Tool**illa, jotka löytyvät NT:n CD-ROM:in **SUPPORT**-hakemistosta.

Vikasietoisuus

Järjestelmän vikasietoisuudella (*Fault Tolerancy*) tarkoitetaan sen kykyä sietää häiriöitä, joiden seurauksena yleensä joko menetetään keskusmuistissa tai kiintolevyillä olevia tietoja tai syntyy laitevaurioita.

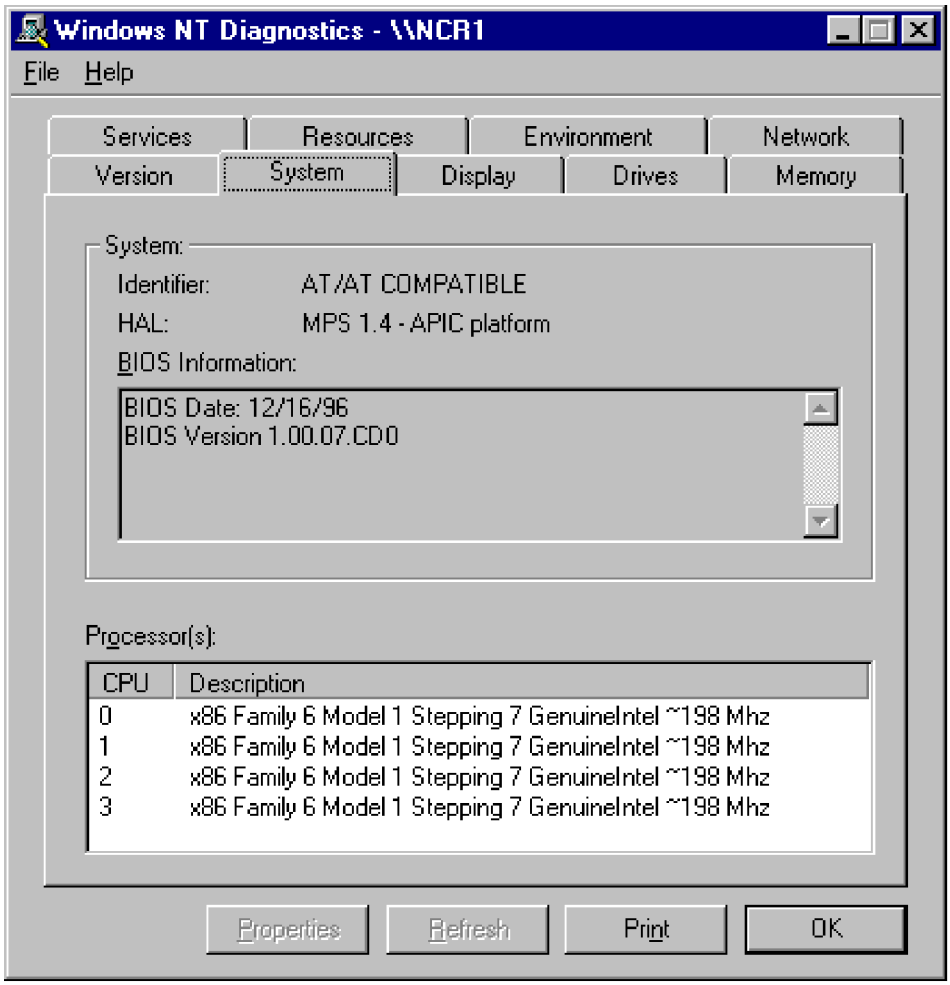
Virransyötön keskeytyminen, kiintolevyn hajoaminen ja tiedostojen korruptoituminen ovat kaikki vikatilanteita, joista **korkean vikasietoisuuden** omaava järjestelmä voi selviytyä ilman että (kaikki) tiedot korruptoituvat. Tyypillisesti koko järjestelmän, mutta erityisesti palvelimen konfiguroinnista riippuu, miten hyvin vakavat virhetilanteet hallitaan. On myös tärkeää konfiguroida vikasietoisuutta lisäävät ominaisuudet usealla eri tasolla eri tyyppisten ongelmien varalle - esimerkiksi UPS-laite virtakatkosten varalle, vikasietoinen levyjärjestelmä levyvikojen varalle jne.

Vaikka tietojen menetys johtuu useimmiten palvelimen levyvioista, se voi olla myös seurausta käyttäjän virheistä, kuten tiedoston tuhoamisesta vahingossa tai viruksen pääsemisestä järjestelmään. Palvelin kannattaa suojata UPS-laitteella, siinä on hyvä käyttää laitteistotasolla levyjen peilausta (*Mirroring*) tai kahdennusta (*Duplexing*). Virustorjuntaa voidaan yksinkertaisimmillaan harjoittaa jopa ottamalla käyttöoikeustarkistukset ja niiden rajoitukset käyttöön.

Prosessori

Pentium Pro- tai **Pentium II**-prosessori ei kaikesta suorituskyvystään huolimatta automaattisesti ratkaise eri laitteistojen pullonkauloja. Esimerkiksi **tiedostopalvelimien** pullonkaulaksi ei yleensä muodostu prosessorin nopeus. Niinpä mikä tahansa **Pentium**-tason (mielellään kuitenkin 133 MHz tai enemmän) laite tyypillisesti käy mainiosti tähän tehtävään.

Tietokantapalvelimet (*Database Server*) ja **Internet-palvelimet** (esimerkiksi *Internet Information Server*) sen sijaan vaativat palvelimelta väntöä - sekä riittävästi keskusmuistia että prosessorin suorituskykyä.



Perinteisesti on sanottu, että uudempi ja nopeampi prosessori on parempi kuin useampi vanhemman sukupolven prosessori. Tämä pätee ainakin Pentium- ja Pentium Pro-prosessoreihin. Yksi Pentium Pro on parempi kuin kaksi Pentiumia. Kaksi- ja neliprosessorisetkin Pentium Pro-palvelimet ovat jo varsin yleisiä.

Muista, että siirryttäessä samassa laitteessa yhdestä prosessorista useampiprosessoriseen järjestelmään tulee Windows NT:n **Hardware Abstraction Layer** (HAL) päivittää vastaavasti.

Moniprosessoripalvelimen on lisäksi syytä noudattaa Intelin **Multiprocessor Specification** (MPS)-standardia. Edelläolevassa esimerkissä standardin versio on **1.4**.

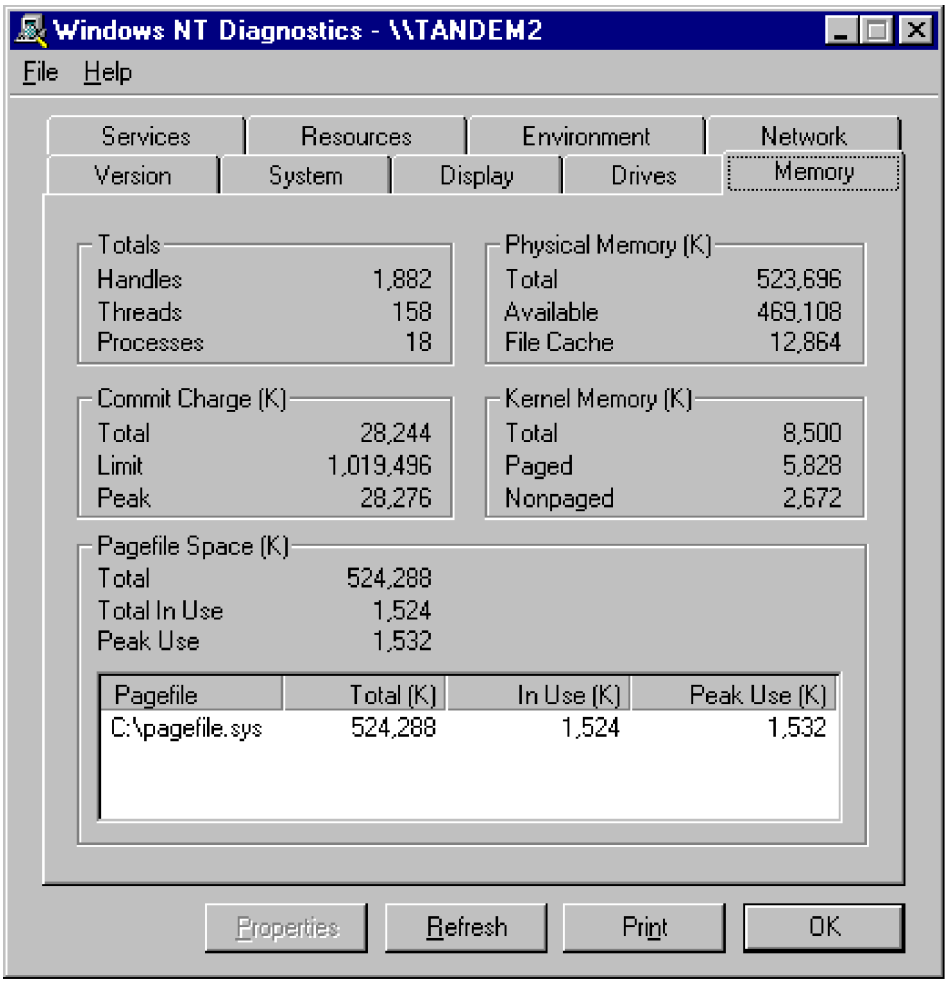
Prosessorien määrän lisäämisessä voi käyttää apuna seuraavaa taulukkoa:

Alkuperäinen lkm	Nykyinen lkm	Suorituskyky
1	2	+95%
2	3	Riippuu järjestelmän kuormituksesta
2	4	+30%
2	6	+50%

Olipa prosessorin nopeus mikä tahansa, se on kuitenkin hidas parin vuoden kuluttua. Tehokäytössä olevan palvelimen käyttöiäksi voi mainiosti laskea 2 - 3 vuotta.

Keskusmuisti

Palvelimet tarvitsevat tyypillisesti paljon keskusmuistia. Muutamien kymmenien käyttäjien **tiedostopalvelimeen** saattaa riittää 32 megatavua, mutta lisättäessä palveluita muistia on ehdottomasti lisättävä. Kirjoittaja ehdottaa aina uuden hankittavan NT-palvelimen muistin määräksi **64 megatavua**. Toki myös ns. päivitettyjen tai muusta käytöstä NT-palvelimiksi siirrettyjen palvelimien muistin määrä riippuu käyttötarkoituksesta, mutta mitä enemmän keskusmuistia on, sitä enemmän NT:n suorituskyky paranee ja koko verkko on tehokkaampi. Suuren verkon monikäyttöpalvelimen (jossa on esimerkiksi **IIS**, **DHCP** ja **WINS**) suositeltavana keskusmuistin minimimääränä voidaan pitää **128 megatavua**.



Tässä esimerkissä keskusmuistia on 512 Mt. Huomaa, että järjestelmälevyllä on vastaavasti sivutustiedoston koko huomattavan suuri (= RAM + 12 Mt)!

Muistin laajennettavuus eri vaihtoehtoineen on syytä selvittää hankinnan yhteydessä. Mitä enemmän muistia, sen tärkeämpiä ovat virheentunnistavat ECC-muistipiirit (*Error-Correction Code*).

Väylä

PCI-väyläarkkitehtuuri on ohittanut EISA-väylän palvelimien standardiväylänä. PCI tarjoaa parhaan suorituskyvyn (132 Mt sekunnissa 33 MHz kellotaajuudella), mutta jos ympäristössäsi on useita EISA-kortteja käyttäviä palvelimia, niin yhteensopivuussyistä palvelimessa *voisi* olla myös tarpeen mukaan muutama EISA-korttipaikka. Mikäli PCI-kortti-

paikkoja tarvitaan useampi kuin kolme tai neljä, tulee laitteessa olla useampia PCI-väyliä. Kaksoisväylärakenne on paras vaihtoehto, mutta myös sillatut ratkaisut toimivat.

Virtalähde

Koska palvelin on verkon tärkein laite, sen virransaanti on varmistettava kaikissa olosuhteissa. Kriittiset komponentit tulisi varmistaa tai kahdentaa. Virransyötössä suositeltavin ratkaisu on vähintään 250 - 300 W virtalähde, joka on kahdennettu.

Näyttö

Vaikka ylellinen värinäyttö ei olekaan Windows NT-palvelimen kannalta välttämättömyys, käyttävät useimmat verkko- ja hallintaohjelmistot eri värejä erilaisten tila- ja virheilmoitusten havainnollistamiseksi, joten minimissään 15-tuumainen, SVGA-tasoinen laite on perusteltu hankinta. Näytönohjaimen muistiksi riittää mainiosti 1 - 2 Mt.

Laitekotelo

Palvelimessa on oltava hyvät laajennusmahdollisuudet. Mikäli laitekotelossa on massamuistipaikkoja yhteensä vähintään kahdeksan, riittää tämä levykeasemaa, CD-ROM-asemaa, tarpeeksi suuren kapasiteetin nauha-asemaa ja neljää kiintolevyä varten. Vapaaksikin jää vielä yksi paikka. Lattialle tai **räkkiin** (*Rack*) sijoitettavaan seisovaan kehikkoon asennettavat kotelot saattavat olla hyvä vaihtoehto ympäristöissä, joissa samoihin tiloihin tulee sijoitettavaksi useita palvelimia (ns. Palvelinhotellit, *Server Hotels*).

Levyjärjestelmä

SCSI-liitäntä (*Small Computer Systems Interface*) mahdollistaa kiintolevyjen lisäksi mm. CD-ROM:ien, optisten lisämuistien ja nauha-asemien liittämisen.

Palvelimissa ei tulisi käyttää muita SCSI-kiintolevyjä. Tähän on useita syitä:

- **Väylänhaltijalaitteet** (*Bus Master*) ovat älykkäitä ja ne hoitavat työn CPU:n puolesta. Prosessori voi jatkaa omia tehtäviään, kun väylänhaltijalaite hoitaa I/O-pyynnöt. Kun I/O-pyynnöt on käsitelty, tulokset palautetaan CPU:lle. **PIO** (*Programmed I/O*) sen sijaan käyttää prosessoria. Siksi useimmissa nopeissa järjestelmissä ei käytetä PIO-laitteita, jotka vaikuttavat tehokkuuteen heikentävästi. PIO-laitteet ovat kuitenkin edullisempia valmistaa ja tavallinen Windows NT:n ATDISK-laiteohjain (IDE-asema) käyttää PIO:a

- Yksi SCSI-ohjain pystyy ohjaamaan seitsemää (tai Wide-SCSI:ssä 15) oheislaitetta ketjutuksen avulla. Lisäksi SCSI-ohjaimia voi olla palvelimessa useampiakin, esimerkiksi yksi (vaikkapa palvelimen emolevylle integroitu) DAT-nauhuria ja CD-ROM:ia varten, toinen (tehokkaampi) kiintolevyjä varten

- SCSI-liitännäiset levyt kykenevät siirtonopeudeltaan 40 Mt nopeuteen

- SCSI-laitteiden keskustelumahdollisuus (*Tag Queuing*) keskenään mahdollistaa nopeamman tietojen käsittelyn ja siirron, jolloin useampi käsky voidaan suorittaa samanaikaisesti. Tällöin esimerkiksi tiedostojen kopiointi kiintolevyltä toiselle voi tapahtua ilman prosessorin ajan tuhlaamista. Prosessori vapautuu muihin tehtäviin välittömästi ja kopioituminen tapahtuu SCSI-ohjainkortin ohjaamana tausta-ajona.

SCSI:stä on tehty kaksi laajennusta: **Wide** ja **Fast**. WideSCSI käyttää 16- tai 32-bitin väylää, jolloin tiedonsiirto on nopeampaa. **Fast** tuplaa kellotaajuuden viidestä kymmeneen megahertsiin ja siten myös tiedonsiirtonopeus tuplaantuu. Molempia voidaan käyttää myös samanaikaisesti. Uusin versio on **UltraSCSI**, joka tukee siirtonopeutta 20 Mt/s Narrow-versiona (*Fast 20*), 40 Mt/s Wide-versiona ja 100 Mt/s valokaapeliversiona (Fiber Channel).

Tunnetuipia SCSI-ohjainkortteja ovat **Adaptec**, **BusLogic** ja **Mylex**. Lisäksi tunnetuilla laitevalmistajilla (esimerkiksi Compaq SmartSCSI) on omia ratkaisuitaan.

Levyjärjestelmän tulisi tarjota RAID-tuki (*Redundant Array of Inexpensive Disks*). Käytetyimmät ovat RAID **0**, **1** ja **5**:

- **RAID 0** jakaa tallennettavan tiedon eri fyysisille levyille. Tällöin käytettävissä on samanaikaisesti useampi luku/kirjoituspää, mikä periaatteessa lisää suorituskykyä. Samalla useamman levyn kapasiteetti voidaan yhdistää - esimerkiksi neljä neljän gigatavun kiintolevyä RAID 0-järjestelmässä tarkoittaa yhteensä 16 gigatavun levyä. RAID 0 ei tarjoa minkäänlaista vikasietoisuutta! Jos yksi kiintolevy vaurioituu, kaikki tiedot menetetään! Varmistusjärjestelmän tulee siis olla entistäkin suorituskykyisempi ja luotettavampi

- **RAID 1** peilaa (*Mirroring*) yhden kiintolevyn tiedot toiselle. Tällöin periaatteessa kahden kiintolevyn järjestelmä kestää yhden kiintolevyn rikkoutumisen, neljän kiintolevyn järjestelmä kahden kiintolevyn rikkoutumisen (jos rikkoutuneet kiintolevyt ovat peilattuja pareja) jne. Peilauksessa puolet kiintolevykapasiteetista menetään peilauksen vuoksi. Peilauksessa voidaan myös käyttää kahta levyohjainta (*Duplexing*), jolloin edes levyohjaimen rikkoutuminen ei keskeytä järjestelmän toimintaa

- **RAID 5** jakaa tallennettavan tiedon eri fyysisille levyille, mutta lisäksi samalla tallennetuista tiedoista tallennetaan XOR-menetelmällä (*Exclusive-OR*) pariteettitarkistus eri kiintolevylle. Tällöin saadaan kahdesta tunnetusta arvosta aina selville puuttuva arvo. Kuten **RAID 0**:ssa, käytettävissä on samanaikaisesti useampi luku/kirjoituspää, mikä lisää suorituskykyä. Laitteistotason vikasietoisuutta (päinvastoin kuin RAID 1:ssä) ei kuitenkaan ole - jos yksi kiintolevy vaurioiutuu, järjestelmä jatkaa toimintaansa, koska tiedot voidaan lukea muilta kiintolevyiltä. Myös RAID 5:ssä useamman kiintolevyn kapasiteetti voidaan yhdistää - esimerkiksi neljä neljän gigatavun kiintolevyä RAID 5-järjestelmässä tarjoaa käyttöön yhteensä 12 gigatavun verran levykapasiteettia.

Kiintolevyn rikkoutumisen varalta kannattaa harkita “lennossa vaihdettavia” (*Hot Swappable*) kiintolevyjä tukevan levyjärjestelmän hankkimista.

Varmistuslaitteet

Digitaaliset nauha-asemat eli DAT-asemat tarjoavat hyvän suorituskyvyn ja yleensä riittävän kapasiteetin varmuuskopioinnin tarpeisiin. Useiden palvelimien varmuuskopiointi voidaan hoitaa kuuden nauhan vaihtimella varustetulla laitteella (*AutoLoader*). Jos kapasiteetti ja/tai teho ei riitä, tarvitaan DLT (*Digital Linear Tape*)-asema. Se tarjoaa pakkaamattomana 15 tai 20 gigatavun kapasiteetin ja pakattuna 30 tai 40 gigatavun kapasiteetin. Kannattaa harkita, ajetaanko varmistukset paikallisesti, kiinteästi asennetulla nauha-asemalla vai verkon kautta. Palvelimiin voidaan lisäksi asentaa erillinen verkkokortti, josta muodostetaan oma verkkonsa ja jonka kautta varmistukset voidaan ajaa verkon kautta.

Tärkeinten palvelimien rekisterit tulisi varmistaa säännöllisesti. Tarkista, että nauhavarmistusohjelmasi tukee rekisterien varmistamista verkon kautta.

CD-ROM

CD-ROM-asemaa tarvitaan Windows NT:n asennuksessa. Jos järjesetlmää joudutaan elvyttämään, myös silloin CD-ROM-asemaa tarvitaan! Aseman tulisi siis olla **kiinteästi palvelimessa**. Mikäli verkossa tarvitaan runsaasti CD-ROM:ille tallennettua tietoa, kannattaa harkita erillisen **Jukebox-CD-ROM-tornin** hankintaa. Tarvittaessa siinä olisi syytä olla **CD-ROM-asemien lukitus**.

Verkkokortti

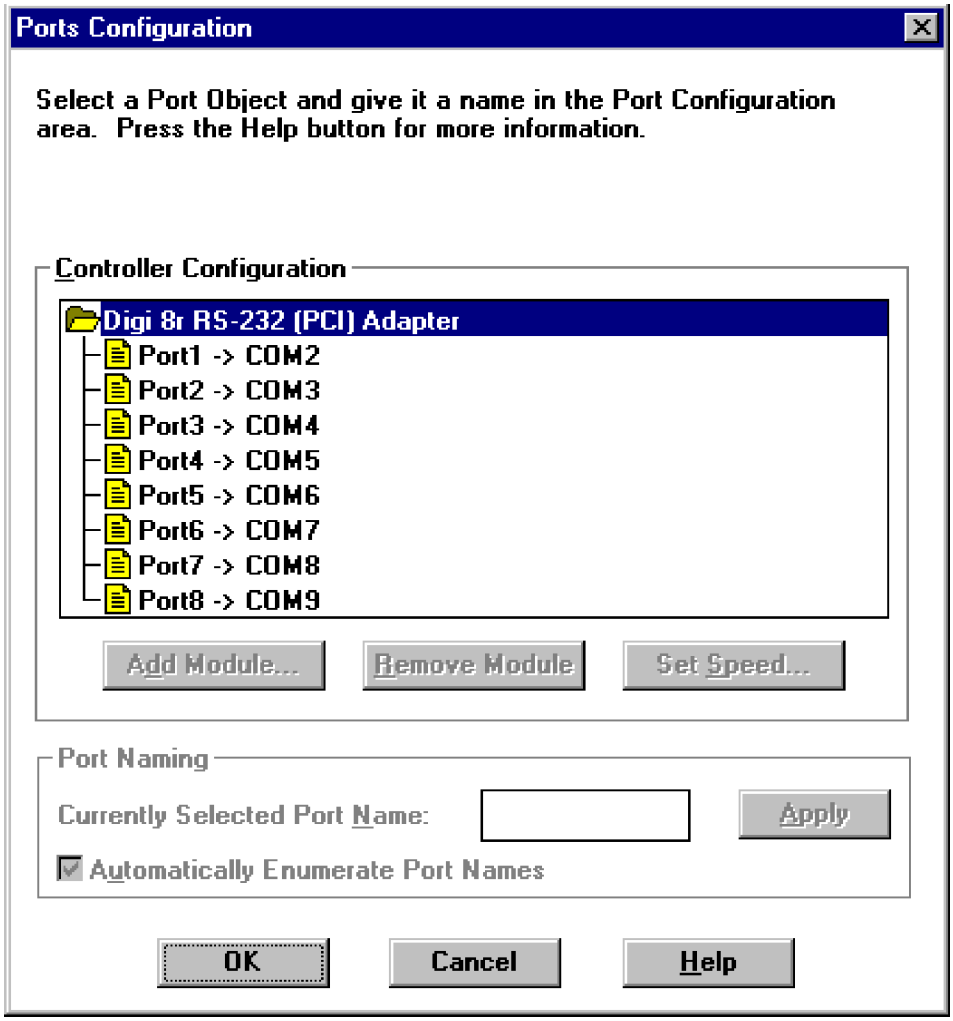
Palvelimeen asennetaan tyypillisesti PCI-väylän Ethernet-verkkokortti. Tyypillisesti palvelimet liitetään **Ethernet-kytkimiin** (*Switch*). Jos verkkokortti ja kytkin tukee kaksisuuntaista toimintatilaa (*Full-Duplex*), palvelimen ja kytkimen välien nopeus voidaan tuplata. Nopeimpia käytännön ratkaisuita tällä hetkellä on 100 megabitin Ethernet (*Fast Ethernet*, 100Base-T).

Jos palvelimeen halutaan useampia verkkokortteja, tarvittaessa voidaan jopa asentaa ns. quad-malli neljän erillisen verkkokortin sijasta: yksi Quad-kortti tukee neljää eri verkkosegmenttiä, joille on kullekin oma liitäntänsä ja osoitteensa.

Modeemi

Palvelimeen voi olla syytä asentaa sisäinen tai ulkoinen modeemi, jonka avulla hallintaohjelmisto voi välittää hälytyksiä pääkäyttäjän hakulaitteeseen ja jonka kautta verkon etähallinta voidaan suorittaa. Eri laitevalmistajilla ja Intelillä on omia ratkaisuitaan.

Etäkäyttöpalvelimen laajennuksessa voi harkita erillisen sarjaporttilaajentimen hankkimista. Tällöin sarjaporttien prosessorilel aiheuttama kuormitus saadaan erilliselle, tavallisesti omalla prosessorillaan varustetulle lisäkortille.



UPS

UPS eli keskeytymättömän virransyötön laite (*Uninterruptible Power Supply*) on välttämätön palvelimen häiriöttömän toiminnan turvaamiseksi. UPS:in merkitys on käytännössä siinä, että sillä kyetään hoitamaan palvelimen hallittu alasajo. UPSin kapasiteetin tulee olla kolmanneksen suurempi kuin palvelimen ja näytön yhteenlaskettu tarve, suuremmat UPSit antavat yleensä enemmän aikaa hallittuun alasajoon. Mikäli laite tarjoaa ohjelmistopohjaiset alasajo-ominaisuudet, kannattaa nämä hyödyntää. Eri laitevalmistajilla on omia ratkaisuitaan.

Windows NT Server

Paitsi laitteiston “raa’an voiman” avulla, myös itse Windows NT-käyttöjärjestelmän avulla voidaan optimoida järjestelmää erilaisiin käyttötilanteisiin sopivaksi.

Sisäänrakennettuna ominaisuutena Windows NT-palvelin- ja -työasemaversiolla on joitakin eroja, jotka eivät ole näkyvissä käyttöliittymän kautta, vaan erot ovat rakennettuja syvälle itse NT-käyttöjärjestelmän konfigurointiin. Tällaisia ovat esimerkiksi:

- Välimuistin levyllekirjoitusmekanismi on suunniteltu erilaiseksi erityyppistä kuormitusta varten
- Palvelinpalvelu (**SRV.SYS**) ei sivuta yhtä innokkaasti palvelinversiossa kuin työasemassa
- Työasemassa Virtual DOS Machine (**VDM**) on esiladattu muistiin sovellusten nopeampaa käynnistämistä varten. Windows NT Server ei esilataa VDM:ää (ei myöskään tyypillisiä työaseman palveluita, kuten **Clipbook Server**iä)
- Säikeiden käsittely on erilainen: Windows NT Server on optimoitu nopeisiin palvelintyyppisiin I/O-toimintoihin ja Windows NT Workstation on optimoitu työasemasovelluksiin
- Windows NT Server voidaan optimoida joko tiedosto- ja kirjoitinpalvelimeksi tai sovelluspalvelimeksi, työasemasta tätä ei voi tehdä käyttöliittymän kautta. Työasemaversio kuitenkin toimii yhtä tehokkaasti kuin palvelinversio noin kymmenelle samanai-

kaiselle tiedosto- ja kirjoitinpalvelintoiminnon käyttäjälle, jolloin pienen vertaisverkon (*Peer-to-peer*) asennus NT-työaseman avulla on mahdollista.

Muistin säätäminen

Muistin riittämättömyys on NT-järjestelmien vakavien ongelmien yleisin syy.

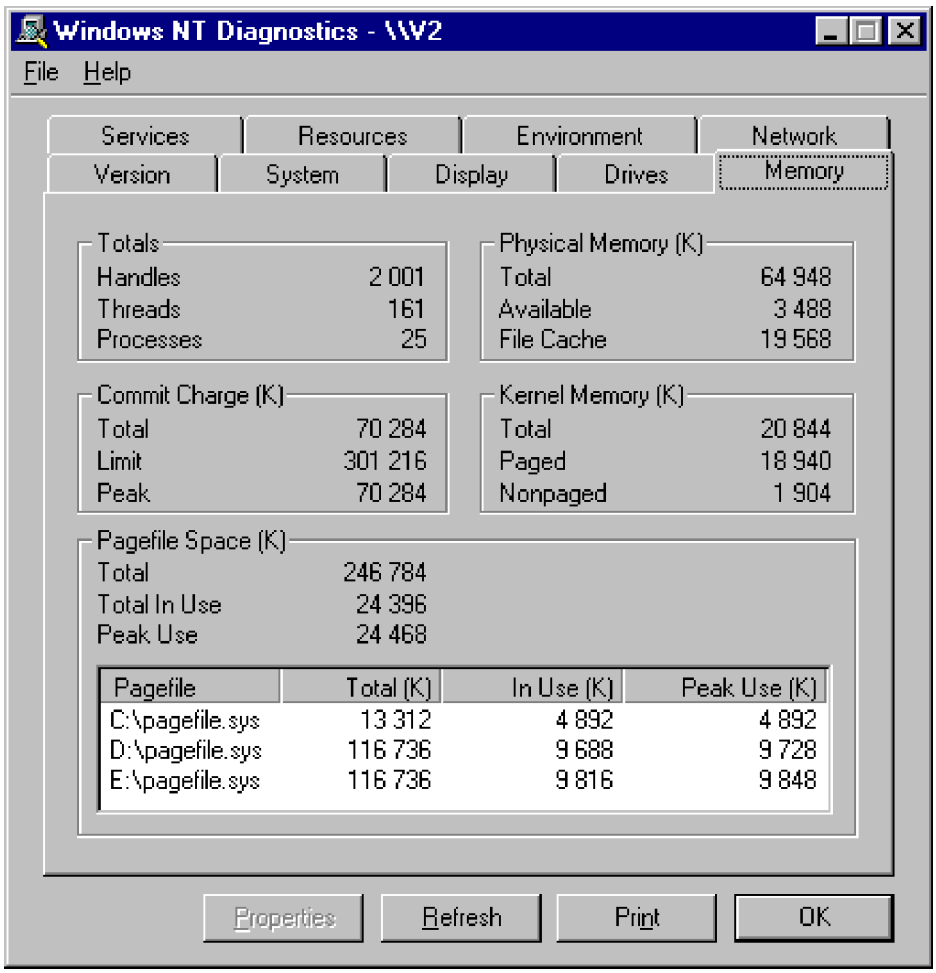
Kilpailu muistiresursseista lisääntyy, kun aktiivisten prosessien muistivaatimukset ylittävät järjestelmän käytettävissä olevan fyysisen muistin ja järjestelmästä **loppuu muisti**. Järjestelmä käsittelee muistin puutteen aloittamalla **sivutuksen** siirtämään osia aktiivisista prosesseista kiintolevylle, jolloin vapautuu fyysistä muistia. Tällöin järjestelmän tehokkuus laskee romahdusmaisesti: jos keskimääräisen käskyn toteuttamiseen kuluu 100 nanosekuntia ja kiintolevyltä lukemiseen kymmeniä millisekunteja, NT-kone toimisi 100 000 kertaa hitaammin, jos jokaista käskyä kohden tarvittaisiin yksi sivutustoiminto!

Kokonaistehokkuuden optimoimiseksi täytyy varmistaa, että keskusmuistia käytetään mahdollisimman tehokkaasti ja sivutuksen tarve pysyy mahdollisimman pienenä. Muistin kuormitustilannetta voi analysoida tarkastelemalla, miten järjestelmä sivuttaa:

- Performance Monitorin laskuri **Memory Pages/sec.** on levyltä luettujen tai sille kirjoitettujen sivujen lukumäärä, kun ratkaistaan muistiviitteitä sivuille, jotka eivät olleet muistissa viittausta tehtäessä. Sääntönä voidaan pitää, että jos laskurin keskiarvo on jatkuvasti yli 5, muistista on tulossa järjestelmän pullonkaula. Kun laskurin keskiarvo alkaa olla 10 tai sen yli, tehokkuus on laskenut huomattavasti ja todennäköisesti tapahtuu *disk thrashing*, jolloin kaikki tehtävät sivutetaan

- Jos sivutustiedoston (**Pagefile.sys**) todellinen koko on suurempi kuin sen **alkuperäinen koko** (*Initial Size*, tyypillisesti RAM + 12 Mt), aikaa kuluu sivutiedoston kasvattamiseen ja tiedoston pirstoutumisesta selviämiseen. Tehokkainta on jos sivutiedoston ei tarvitse kasvaa järjestelmän toimiessa, koska silloin sivutusprosessiin kuluu enemmän aikaa (lisää levyhakuja tarvittavien sektorien varaamiseen, allokointien päivitys ja vieläpä eri tiedostojärjestelmien vapaiden sektorien käsittely). Toinen seuraus

tästä on pirstoutuminen (*Fragmentation*), jolloin sivutustiedosto sijaitsee monissa paikoissa kiintolevyllä (alkuperäistä sivua käytetään rinnakkaisen levytilan luomiseen)



Nopea tapa saada selville, onko järjestelmässä muistiongelmia on **Windows NT Dignostics**in **Memory**-välilehti sekä **Performance Monitor**:

- **Physical Memory** | **Available Bytes** näyttää vapaan fyysisen muistin määrän. Jos laskurin arvo pysyy jatkuvasti 1 Mt:n alapuolella palvelimilla ja 4 Mt:n alla työasemilla, tapahtuu sivutusta ja tehokkuus ei ole paras mahdollinen

- **Commit Charge** | **Total** näyttää käytetyn virtuaalimuistin koon tavuissa. Jos laskurin arvo on suurempi kuin keskusmuisti, keskusmuisti ei ehkä ole riittävä kaikille aktiivisille prosesseille – jonkin verran sivutusta on kuitenkin väistämätön. On myös syytä tarkistaa Performance Monitorin **Memory Pages/sec** ja **Memory Page Faults/sec**. Jos **Memory Pages/sec** on suurempi

kuin **10** (arvo vaihtelee levyjärjestelmän mukaan) ja **Memory Page Faults/sec** on suurempi kuin **Memory Cache Faults/sec**, sivutusta tapahtuu liikaa

- Jos haluat selvittää, olisiko muistin lisäämisestä hyötyä **Microsoft SQL Server**ille, kannattaa seurata arvoa **SQL Server Cache Hit Ratio**, kun järjestelmää kuormitetaan normaalisti. Jos välimuistin osumasuhde on melko korkea (yli 90%), muistin lisääminen ei tavallisesti auta. Tämä johtuu siitä, että lisämuistia voidaan käyttää lähinnä Microsoft SQL Serverin välimuistin kasvattamiseen, jolloin osumasuhde kasvaa entisestään. Tässä tapauksessa osumasuhde on jo korkea ja suurin saavutettava parannus melko pieni

- Kun **Commit Charge** saavuttaa arvon **Limit** – ja sivutustiedoston koko on jo saavuttanut sivutustiedoston maksimikoon, lisäsivuja ei yksinkertaisesti ole saatavilla. **Limit** on se virtuaalimuistin määrä, joka voidaan tarjota ilman sivutustiedoston jatkamista. Jos näin käy, Windows NT Server -palvelimella, tapahtumalokiin voi odottaa kolmea virheilmoitusta lähteestä (*Source*) **SRV:**

  2020: The server was unable to allocate from the system nonpaged pool because the pool was empty

  2001: The server was unable to perform an operation due to a shortage of available resources

  2016: The server was unable to allocate virtual memory.

Jos näin käy, se tavallisesti se liittyy muistiongelmiin jossakin toisessa prosessissa. Prosessi voidaan löytää tutkimalla kunkin prosessin **Page File Bytes**- tai **Working Sets** -arvoja.

Toinen tilanne on palvelimen tapahtumalokin seuraava sivuttamaton muistivirhe (*NonPaged Pool*):

> **2019: The server was unable to allocate from the system nonpaged pool because the pool was empty**

Tällöin sivuttamatonta muistia ei voida sivuttaa sivutustiedostoon, vaan se pysyy keskusmuistissa kunnes se allokoidaan.

NonPagedPoolSize (sivuttamattoman muistin koko) lasketaan fyysisestä muistista monimutkaisilla algoritmeilla. Arvoa voidaan kuitenkin hakea Intel x86-pohjaisille NT-koneille seuraavasti:

- MinimumNonPagedPoolSize = 256k (sivuttamattoman muistin minimikoko)
- MinAdditionNonPagedPoolPerMB = 32k (sivuttamattoman muistin minimilisäys / Mt)
- DefaultMaximumNonPagedPool = 1 Mt (sivuttamattoman muistin oletusmaksimikoko)
- MaxAdditionNonPagedPoolPerMB = 400 kt (sivuttamattoman muistin max. lisäys / Mt)
- PAGE_SIZE = 4096

Algoritmi on **NonPagedPoolSize** = MinimumNonPagedPoolSize + ((Fyysiset Mt - 4) * MinAdditionNonPagedPoolPerMB)

Esimerkiksi 32 Mt Intel x86-pohjaisella NT-koneella:

MinimumNonPagedPoolSize = 256k

NonPagedPoolSize = 256k + ((32 - 4) * 32k) = **1,2 Mt** (= sivuttamattoman muistin koko)

Algoritmi, jolla lasketaan maksimi sivuttamattoman muistin koko, on **MaximumNonPagedPoolSize** = DefaultMaximumNonPagedPool + ((Fyysinen Mt - 4) * MaxAdditionNonPagedPoolPerMB)

Jos MaximumNonPagedPoolSize < (NonPagedPoolSize + PAGE_SIZE * 16), **niin** MaximumNonPagedPoolSize = (NonPagedPoolSize + PAGE_SIZE * 16).

Edellisen esimerkiksi NT-koneessa **MaximumNonPagedPoolSize** = 1 Mt + ((32-4) * 400 k) = **12,5 Mt** (maksimi sivuttamattoman muistin koko).

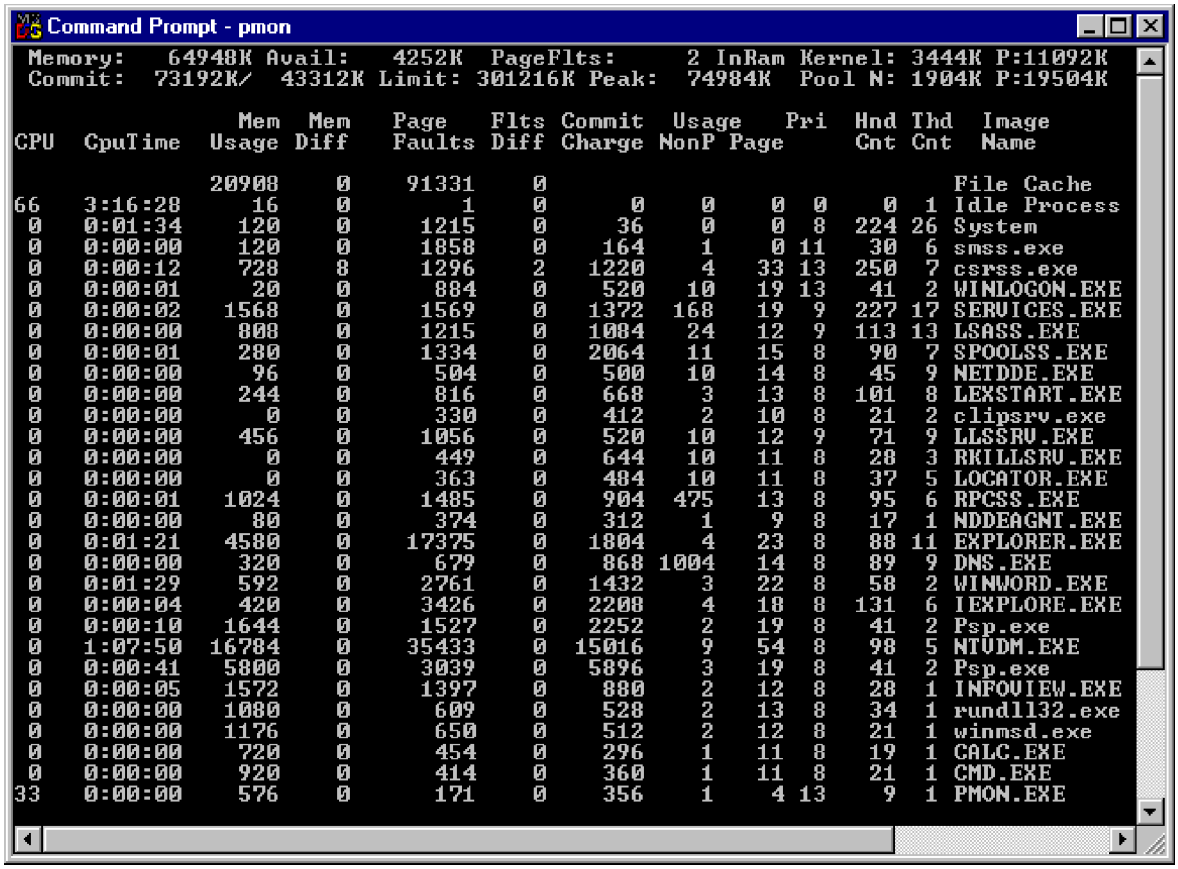
Järjestelmän sivuttamattoman muistin allokointia voidaan seurata laskurista **Memory** | **Pool Non Paged Bytes**. Jos sivuttamattomasta muistista on pulaa, voidaan saada myös seuraava virheilmoitus:

Not enough storage available to process this command

Jos näin käy, tutki jokaisen prosessin sivuttamattoman muistin allokointia. Tavallisesti ilmoitus johtuu siitä, että järjestelmä tekee virheellisiä järjestelmäkutsuja ja käyttää loppuun kaiken allokoidun sivuttamattoman muistin.

Jos arvelet, että yksi sovellus kuluttaa suuren osan muistista (sivutetusta tai sivuttamattomasta), sen järjestelmälle aiheuttamaa kuormaa voi seurata esimerkiksi Resource Kitin **PMON.EXE**-apuohjelmalla. Samat tiedot saa Performance Monitorin laskureista (esimerkiksi **Page Faults/sec**) ja Task Managerista, mutta tässä tiedot on koottu valmiiksi yhteen.

PMON-näytön yläosassa on joitakin yleistietoja järjestelmästä: muistin ja käytettävissä olevan muistin koko tavuina, virtuaalimuistin varatun määrän sekä muistien koot.



Sitten PMON näyttää jokaiselle prosessille suorittimen käyttömäärän (**%CPU**) viimeisen päivityksen jälkeen. Seuraavassa sarakkeessa on kokonaissuoritinaika (**CpuTime**). Sarakkeesta **Page Faults** näkyy, montako sivutusvirhettä prosessissa on tapahtunut ja seuraavasta sarakkeesta muutos edelliseen päivitykseen (**Flts Diff**) verrattuna. Seuraavana on virtuaalimuistissa varattu koko ja prosessin muistin käyttöarviot. Lopuksi näytetään prosessin prioriteetti (**Pri**) ja säikeiden lukumäärä (**Thd Cnt**).

Vinkkejä:

- Siirrä - jos mahdollista - paljon muistia vaativat sovellukset ruuhka-ajan ulkopuolelle AT-komennolla
- Jaa paljon muistia tarvitsevat sovellukset/prosessit useille eri NT-palvelimille (RAS, WINS jne)
- Lisää muistin määrää. Määritä seuraavan kaavan avulla, kuinka paljon suunnilleen tarvitset lisämuistia: **Paging File** | **%Usage Max** eli sivutustiedoston käytössä olevien tavujen määrä
- Laske kaikkien sivutustiedostojen käyttämät tavumäärät yhteen.

Tämä muistin määrä tarvitaan lisää, jotta kaikki sovellukset voisivat suorittaa tehtävänsä mahdollisimman vähäisellä sivutuksella. Jos esimerkiksi sivutiedoston koko on **200 Mt** ja **%Usage Max** on **20%**, tarvitaan **40 Mt** lisää RAM:ia, jotta järjestelmä sivuttaisi mahdollisimman vähän. Koko sivutustiedoston käytössä olevaa koodia ei käytetä kaiken aikaa ja kaavassa ei oteta huomioon sivutustiedoston käsittelyn ulkopuolella olevia ohjelmatiedostoja. Siksi arvio on vain suuntaa-antava

- **Sivutustiedostojen** levittäminen useille kiintolevyille ja levyohjaimille parantaa tavallisesti tehokkuutta, koska levyt voivat käsitellä I/O-pyyntöjä yhtäaikaisesti. Käytössä voi kuitenkin olla enintään 16 erillistä sivutustiedostoa. Koska Windows NT:ssä on monia usein käytettyjä järjestelmätiedostoja, kannattaa kokeilla sivutustiedoston sijoittamista muille kuin Windows NT-järjestelmätiedostojen levylle. Sivutustiedosto(t) pitäisi myös sijoittaa eri kiintolevy(i)lle kuin sovellustiedostot, jolloin sivutustiedosto-I/O ja sovellustiedosto-I/O voi tapahtua samanaikaisesti. Tämä onnistuu vain, jos levyajuri(t) ja ohjain(ohjaimet) pystyvät käsittelemään **asynkronisia I/O-pyyntöjä**. IDE-kiintolevyjen käyttämässä **ATDISK**-laiteohjain pystyy käsittelemään vain yhden I/O-pyynnön kerrallaan. Jos järjestelmässä käytetään sekä nopeita että hitaita levyjä, käytä kaikkeen sivutukseen nopeimpia levyjä

- Käytä **Control Panel** | **System** | **Performance**-välilehteä määrittääksesi sivutiedoston koon sellaiseksi, että sen koko ylittyy harvoin

- Valitse **Control Panel** | **Services** ja sammuta **tarpeettomat** Windows NT -palvelut, ja **Control Panel** | **Network** poistaaksesi tarpeettomat Windows NT -laiteohjaimet ja -palvelut

- Käyttäjätunnuksia säilytetään rekisterissä, jolloin jokainen käyttäjätunnus käyttää PDC:n tai BDC:n sivutettua muistia. Käyttäjätunnusten maksimimäärä riippuu siis palvelinten keskusmuistin määrästä ja sivutustiedoston koosta. Yksi käyttäjätunnus vie tilaa n. 1 kt ja 10000 tunnusta siis n. 10 Mt. Näin ollen suorituskykysyistäkin kyseeseen saattaa tulla toisenlainen toimialuemalli, jos käyttäjiä on esimerkiksi yli 15000. Muistin lisääminen voi kuitenkin olla helpoin ratkaisu.

- Toinen menetelmä mitata sovelluksen tarvitseman muistin määrää on ajaa sovellusta *varmasti* riittävällä muistilla ja mitata muistin tarvetta vähäisellä muistin kuormituksella. Apuna voi käyttää Resource Kitin **PROBE**-apuohjelmaa

- Vanhemmissa palvelimissa muistin lisääminen ilman **Level 2**-välimuistin lisäämistä *saattaa* heikentää joskus suorittimen tehoa. Tämä johtuu siitä, että Level 2- välimuistin täytyy nyt tunnistaa laajempi muistiavaruus, jolloin välimuistissa saavutetaan tavallisesti heikompi osumasuhde. Tällöin paljon prosessoria käyttävät ohjelmat saattavat hidastua, koska ne ovat muistissa laajemmalla alueella. Ero menee hiustenhalkomiseksi, jos Level 2-välimuisti on itse prosessorissa

- Joissakin koneissa on *ROM BIOS Shadowing* -mahdollisuus. Se on menetelmä, jossa BIOS kopioidaan ROM:ista RAM:iin. Koska RAM:in lukeminen on selvästi nopeampaa kuin ROM:in lukeminen, paljon BIOS:ia käyttävät toiminnot nopeutuvat merkittävästi. Esimerkiksi MS-DOS käyttää BIOS:ia näytön kirjoittamiseen ja siksi MS-DOS-järjestelmä voi nopeutua tällä menetelmällä. Windows NT **ei** käytä BIOS:ia (paitsi käynnistysvaiheessa) eikä tehokkuus siksi parane tällä menetelmällä. Jos ROM BIOS Shadowing ei ole käytössä, käytettävissä on enemmän RAM-muistia.

Prosessorin tehokkuuden säätäminen

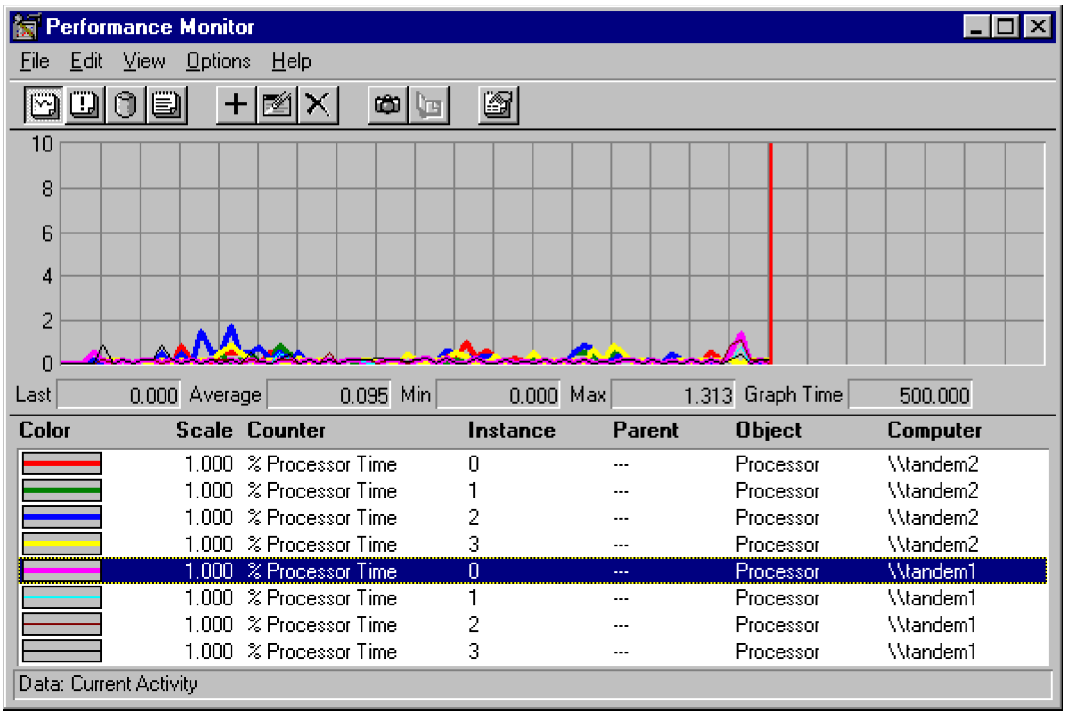
Prosessori voi toteuttaa tietyn määrän käskyjä (kellotaajuus) sekunnissa. Kun prosessoria käytetään useiden säikeiden ajamiseen, tietyn säikeen ajamiseen kuluu x kertaa (jossa x on samanaikaisesti ajettavien säikeiden määrä) kauemmin tietyn tehtävän tekemiseen.

Säikeellä ei tiettyinä aikoina ole tehtäviä, esimerkiksi kun se odottaa käyttäjän syötettä tai kun se odottaa, että jokin toinen säie lopettaa säikeeseen liittyvän tehtävän. Kun säie on odotustilassa, sitä ei suunnitella ajettavaksi eikä se siksi kuluta suorittimen aikaa. Koska useimmissa Windows-sovelluksissa kuluu huomattavan paljon aikaa odotustilassa oleviin säikeisiin, tehokkuus saattaa laskea vain vähän, kun ajetaan useita Windows-pohjaisia sovelluksia.

Jotkin sovellukset käyttävät paljon suoritinaikaa: niillä on lähes aina tehtäviä ja ne kuluttavat vähän tai eivät yhtään aikaa odotustilassa.

Resource Kitin mukana tulee **P5Ctrs**, jolla saadaan Pentium/Pentium Pro-prosessorien sisäiset laskurit Performance Monitorin käyttöön.

Jos laskurin **Processor** | **%Processor Time** arvo on jatkuvasti **100 %** tai lähellä sitä, suoritin voi olla pullonkaula. Moniprosessorijärjestelmissä seurataan laskuria **System** | **%Total processor time**. Tässä on kyseessä kaksi neliprosessorikonetta:



Seurattavia kohteita:

- Haluttaessa selvittää kuluttaa prosessoritehoa tutkitaan eniten prosessorin aikaa kuluttava prosessi seuraamalla eri tapauksia **Process** | **%Processor Time** -laskurissa.

- Seuraamalla arvoa **Processor** | **Interrupts/sec.** voidaan määrittää, johtuuko prosessorin toiminta sovelluksista vai laitteistokeskeytyksistä. Arvo kertoo, montako laitteistokeskeytystä suorittimeen tulee sekunnissa. Jos se on yli **1000**, kannattaa tarkistaa I/O-laitteiden, esimerkiksi levyohjainten ja verkkokorttien tehokkuus.

- Seuraa myös arvoa **System | System Calls/sec.**. Järjestelmäkutsuja/sekunti on taajuus, jolla Windows NT -järjestelmäpalvelurutiineja kutsutaan. Rutiinit hoitavat perusaikataulutuksen ja NT-koneen toimintojen tahdistamisen sekä tarjoavat mm. pääsyn muistin hallintaan. Jos keskeytyksiä on sekuntia kohden paljon enemmän kuin järjestelmäkutsuja, jokin laite saattaa aiheuttaa liian paljon keskeytyksiä

- Seuraa myös arvoa **System | Context Switches/sec.**. Liian tiheät prosessorin tilanvaihdot (*context switching*) voivat tapahtua, jos järjestelmän semaforit (*Semaphors*) tai kriittiset lohkot (*Critical Sections*) on sijoitettu liian alhaiselle tasolle (*Kernel Modeen*) tehokkaan samanaikaisuuden saavuttamiseksi. Ainoa tapa ratkaista tämä ongelma on lähdekoodissa.

Vinkkejä:

- Siirrä paljon prosessoriaikaa vaativat sovellukset ajettaviksi esimerkiksi yöllä (jos mahdollista). Apuna voit käyttää AT-komentoa

- Jaa sovellukset ja prosessit useille eri palvelimille

- Vaihda prosessori uudempaan, jos mahdollista. Useimmat palvelimet ovat **joko** tiedosto- tai sovelluspalvelimia. Vaikka ne käyttävät samaa käyttöjärjestelmää, ne käyttävät koneen resursseja eri tavalla. Tiedostopalvelin pyrkii yleensä maksimoimaan järjestelmäväylän käytön ja käyttää suoritinaikaa vähemmän. Sovelluspalvelin (esimerkiksi Microsoft SQL Server ja Systems Management Server) käyttää kuitenkin prosessoria huomattavasti enemmän kuin tiedostopalvelimet. Tällaisessa ympäristössä on hyötyä tehokkaammasta prosessorista

- Lisää prosessorien määrää, jos enemmän kuin yksi säie pystyy asynkroniseen ajoon. Jos palvelimessa on useita suorittimia, Windows NT määrittää eri säikeet eri suorittimille sekä myös keskeytykset jaetaan prosessorien kesken. Säikeiden ajokuorma jakautuu prosessorien kesken. Jos esimerkiksi paljon prosessoriaikaa käyttävää säiettä ajetaan 0-prosessorilla, 1-prosessori on vapaa muiden säikeiden ajamiseen

- Jos lisäkortissa ei suoraa muistinsiirtoa (*Direct Memory Addressing*, DMA), se käyttää prosessoria tietojen siirtämiseen,

jolloin prosessorille tulee lisäkuormitusta. PIO-laitteiden korvaaminen poistaa tehokkaasti prosessoreista johtuvia pullonkauloja

- Voit muuttaa **START**-komennolla ohjelman prioriteettia käynnistettäessä sitä. Komennon valitsimet ovat **/low**, **/normal**, **/high** ja **/realtime**, ja niiden avulla voidaan käynnistää ohjelmia eri prioriteettitasoilla. Älä koskaan käynnistä huomattavasti prosessoriaikaa vaativia sovelluksia realtime-prioriteetilla!

Levyjärjestelmän tehokkuuden säätäminen

Kiintolevyn toiminta on tärkein yksittäinen tekijä I/O-laitteiden tehokkuudessa, koska tehokas levyjärjestelmä parantaa virtuaalimuistin toimintaa ja vähentää aikaa, joka tarvitaan paljon I/O:ta tarvitsevien ohjelmien lataamiseen. Jos levyjärjestelmä on pullonkaula, täytyy ensin selvittää, tarvitaanko itse asiassa lisää keskusmuistia. Jos muistia on vähän, tehokkuuden heikkeneminen voi heijastua myös levypullonkaulana.

Windows NT ei aktivoi levynseurannan laskureita automaattisesti järjestelmän käynnistysvaiheessa. Levylaskurit voi aktivoida komentorivin komennolla **diskperf -y** ja käynnistämällä NT-koneen uudelleen.

Seurattavia kohteita:

- Jos laskurin **Physical Disk** |**%Disk Time** arvo on jatkuvasti **100 %** tai lähellä sitä, fyysinen levy on pullonkaula. Laskuri näyttää käytetystä ajasta prosenttiarvon, jonka levyajuri palvelee luku- tai kirjoituspyyntöjä

- Jos laskurin **Physical Disk** | **Disk Queue Length** (odottamassa olevat levy-I/O-pyynnöt) arvo on suurempi kuin **2**, levy on ruuhkainen. Sama pätee useimpiin muihinkin I/O-laitteisiin

- Levy-I/O:sta sivutukseen käytetty osa selviää kaavalla **% sivutukseen käytetty levyaika = 100 * (Memory Pages/sec * Physical Disk Avg.DiskSec/Transfer)**. Jos arvo on yli **10 %** kokonaislevytoiminnasta, sivutusta tapahtuu liikaa. **Avg.DiskSec/Transfer** on keskimääräiseen levysiirtoon kuluva aika.

Vinkkejä:

- Kiintolevyn tiedostot pirstoutuvat (*Fragmentation*) aikaa myöten, mikä tarkoittaa sitä, että tiedostojen osia levitetään levylle eri alueille. Järjestelmä ei löydä riittävästi vierekkäisiä lohkoja, jotta uusi tiedosto voitaisiin tallentaa yhteen paikkaan ja sen täytyy siksi sijoittaa tiedosto muiden tiedostojen välissä oleviin tyhjiin tiloihin. Kun tiedostoja lisätään, poistetaan ja laajennetaan, levyn tiedostot pirstoutuvat yhä enemmän. Tehokkuus kärsii, koska tiedostoa ei pystytä lukemaan peräkkäisillä toiminnoilla. Käytä pirstoutumisen estämiseksi Defrag-apuohjelmaa tiedostojen järjestämiseen, esimerkiksi Executive Softwaren **DiskKeeper** -ohjelmaa (**http://www.execsoft.com**) tai Nortonin Speed Diskiä (**http://www.symantec.com**)

- NTFS on tyypillisesti paras tiedostojärjestelmä yli 400 Mt:n levyillä. Tehokkuus ei laske levykoon kasvaessa NTFS:ää käytettäessä, toisin kuin FAT-tiedostojärjestelmässä. Tähän vaikuttaa mm. tilanvarausyksikön koko. FAT-tiedostojärjestelmässä tiedostojen vaatima levytila on suurempi kuin NTFS:ää käytettäessä:

Levyosion koko	FAT	NTFS
< 128 Mt	2 kt (2048 t)	512 t
129 Mt < 256 Mt	4 kt (4096 t)	512 t
257 Mt < 512 Mt	8 kt (8192 t)	512 t
513 Mt < 1024 Mt (1 Gt)	16 kt (16384 t)	1 kt (1024 t)
1025 Mt < 2048 Mt (2 Gt)	32 kt (32768 t)	2 kt (2048 t)
2049 Mt < 4096 Mt (4 Gt)	-	4 kt (4096 t)
4097 Mt < 8192 Mt (8 Gt)	-	8 kt (8192 t)
8193 Mt < 16384 Mt (16 Gt)	-	16 kt (16384 t)
16385 Mt < 32768 Mt (32 Gt)	-	32 kt (32768 t)
> 32768 Mt	-	64 kt (65536 t)

- Lyhyiden nimien luomisen estäminen NTFS-partitiossa parantaa huomattavasti hakemistojen luettelemisnopeutta varsinkin, jos hakemistoissa on paljon tiedostoja/hakemistoja, joilla on pitkät tiedostonimet. Lyhyiden tiedostonimien luomisen voit estää rekisterissä:

Polku	**HKEY_LOCAL_MACHINE\SYSTEM**
Avain	**\CurrentControlSet\Control\FileSystem**
Nimi	**NtfsDisable8dot3NameCreation**
Tyyppi	**REG_DWORD**
Arvo	**0 - luodaan lyhyet tiedostonimet (oletus), 1 - ei luoda**

Tästä voi tosin seurata yhteensopivuusongelmia 16-bittisten MS-DOS- ja Windows-sovellusten kanssa.

Palvelinlaitteistoja

Seuraavassa on yhteenvedon omaisesti joidenkin valmistajien palvelinlaitteistoja. Laitteet ovat aakkosjärjestyksessä.

Compaq ProLiant 6000

Compaq ProLiant 6000	
Suorituskyky	CPU: Pentium Pro / 200 MHz Kaksi Ultra Fast/Wide SCSI-kanavaa Kaksi PCI-väylää
Skaalattavuus	1 - 4 prosessoria (512 kt) Level 2-välimuistilla 4 Gt RAM 5 PCI-korttipaikkaa 2 jaettua korttipaikkaa 1 EISA-korttipaikka 109,2 Gt sisäinen levymuisti 937,3 Gt ulkoinen levymuisti
Hallinta	SmartStart Insight Manager Remote Insight Board
Vikasietoisuus	Varavirtalähde ECC-muisti Hot-swap-levyt Online Recovery Server

Digital Prioris 6000 ZX

Digital Prioris 6000 ZX	
Suorituskyky	CPU: Pentium Pro / 200 MHz Kaksi Fast/Wide SCSI-kanavaa Kaksi PCI-väylää
Skaalattavuus	1 - 4 prosessoria (512 kt) Level 2-väli-muistilla 2 Gt RAM 12 laajennuskorttipaikkaa (joista 8 PCI-korttipaikkaa) 28 Gt sisäinen levymuisti 1 Tt ulkoinen levymuisti
Hallinta	ServerWorks Quick Launch ServerWorks Manager Remote Server Manager
Vikasietoisuus	Varavirtalähteet Tuulettimet ECC-muisti Hot-swap-levyt Digital Cluster for NT

HP NetServer LX Pro

HP NetServer LX Pro	
Suorituskyky	CPU: Pentium Pro / 200 MHz Kaksi Fast/Wide SCSI-kanavaa Kaksi PCI-väylää
Skaalattavuus	1 - 4 prosessoria (512 kt) Level 2-väli-muistilla 2 Gt RAM 10 laajennuskorttipaikkaa (joista 6 PCI-korttipaikkaa) 109 Gt sisäinen levymuisti
Hallinta	NetServer Navigator OpenView for Windows Remote Assistant
Vikasietoisuus	Tuulettimet ECC-muisti Hot-swap-varavirtalähteet Hot-swap-levyt

IBM Server 704

IBM Server 704	
Suorituskyky	CPU: Pentium Pro / 200 MHz Kaksi Fast/Wide SCSI-kanavaa Kaksi PCI-väylää
Skaalattavuus	1 - 4 prosessoria (512 kt) Level 2-välimuistilla 2 Gt RAM 10 laajennuskorttipaikkaa (joista 6 PCI-korttipaikkaa) 48 Gt sisäinen levymuisti
Hallinta	NetFinity 4.0
Vikasietoisuus	ECC-muisti Varavirtalähteet Hot-swap-levyt

NCR 4300

NCR 4300	
Suorituskyky	CPU: Pentium Pro / 200 MHz Kaksikanavainen Ultra Fast/Wide-SCSI-ohjain Nelikanavainen PCI SCSI-ohjain Kaksi PCI-väylää
Skaalattavuus	1 - 4 prosessoria (512 kt) Level 2-välimuistilla 2 Gt RAM (4 Gt DIMM) 6 PCI-korttipaikkaa 4 EISA-korttipaikkaa 54 Gt sisäinen levymuisti (á 9 Gt)
Hallinta	Server Management-prosessori
Vikasietoisuus	ECC-muisti Hot-swap-varavirtalähteet Hot-swap-levyt Sisäinen SMP-klusteri LifeKeeper Ulkoiset RAID-ohjaimet

Tandem S1000

Tandem S1000	
Suorituskyky	CPU: Pentium Pro / 200 MHz Kaksikanavainen Ultra Fast/Wide-SCSI-ohjain Nelikanavainen PCI SCSI-ohjain Kaksi PCI-väylää
Skaalattavuus	1 - 4 prosessoria (512 kt) Level 2-välimuistilla 1 Gt RAM (4 Gt DIMM) 4 PCI/EISA-korttipaikkaa 1 EISA-korttipaikkaa 9 levypaikkaa, joista 6 Hot-Swap 54 Gt sisäinen levymuisti (9 Gt levyillä)
Hallinta	LANDesk Server Management Solution
Vikasietoisuus	ECC-muisti Varavirtalähteet Hot-swap-levyt Ulkoiset RAID-ohjaimet

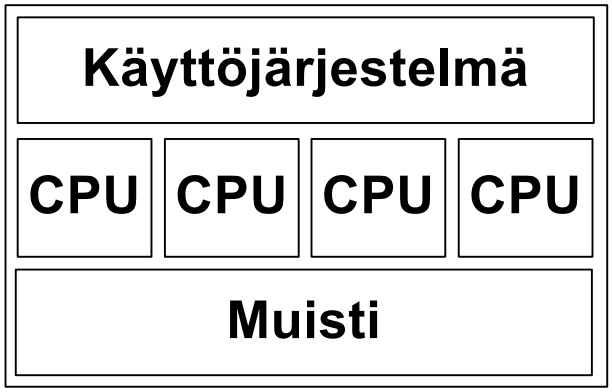
Klusterit

Klusteri (Cluster, myös **ryväs**) on joukko toisiinsa liitettyjä tietokoneita (Loosely Coupled), joka toimii yhtenä järjestelmänä. Järjestelmän käyttäjien kannalta järjestelmä näyttää yhdeltä suorituskykyiseltä, vikasietoiselta palvelimelta.

Käsitteitä

Klusterointi voi tarkoittaa monia asioita. Seuraavaksi peruskäsitteitä aiheen ympäriltä:

- **Symmetric Multiprocessing** - yksi menetelmä skaalattavuuden lisäämisessä tietokonejärjestelmissä on ollut prosessorien lisääminen. Symmetrisissä moniprosessorijärjestelmissä (*Symmetric Multiprocessing*, SMP) prosessorit ovat samanlaisia, ja jakavat yhteisen muistiavaruuden ja I/O-järjestelmän. Windows NT tukee SMP-menetelmää, ja on saatavissa on jopa kahdeksan prosessorin (*Eight-Way*) järjestelmiä (epäsymmetrisessä moniprosessorijärjestelmissä erilaiset prosessorit hoitavat eriytyneitä tehtäviä). Ongelmaksi muodostuu palvelimen sisäiset väylät, I/O jne



- **Shared Memory Model** -malli liittyy SMP-menetelmään, jossa käyttöjärjestelmästä ajetaan yhtä kopiota. Jos ajettavat sovellukset *eivät* käytä yhteistä dataa, järjestelmä on tehokas

- **Shared Nothing** -mallissa jokainen klusterin osa omistaa omat resurssinsa. Vain yksi järjestelmän osa - se, joka omistaa resurssin - pääsee käsiksi resursseihinsa. Vikatilanteessa toinen klusterin osa ottaa resurssin omistukseensa ja käyttäjien kyseiseen resurssiin kohdistamat pyynnöt ohjataan oikealle resurssin omistajalle.

Shared Disk Model -mallin lisäksi myös **Shared Nothing** -malli on osa nykyaikaista klusterointitekniikkaa, ja ne voivat olla samanaikaisesti käytössä samassa klusterissa. Tällöin sovellukset, jotka esimerkiksi pääasiassa lukevat levyillä olevaa dataa, voivat käyttää **Shared Disk Model** -mallia ja skaalautuvat sovellukset käyttävät **Shared Nothing** -mallia.

Näistä voidaan käyttää klusteroinnissa myös käsitteitä **Fail-over** ja **Parallel Applications**:

- **Fail-over** tarkoittaa sovellusten nopeaa käynnistämisestä varapalvelimelta, jolloin käytettävyys paranee (*High-Availability*). Se ei sinällään vaikuta **skaalautuvuuteen** ja vikatilanteesta elpyminen saattaa kestää 15 - 30 sekuntia (riippuen toki palvelusta)

- **Parallel Applications** tarkoittaa sovellusten jakamista useammalle palvelimelle. Tällöin saadaan lisää suorituskykyä, ja yhden prosessin kaatuessa se siirretään toiselle palvelimelle.

Ominaisuuksia

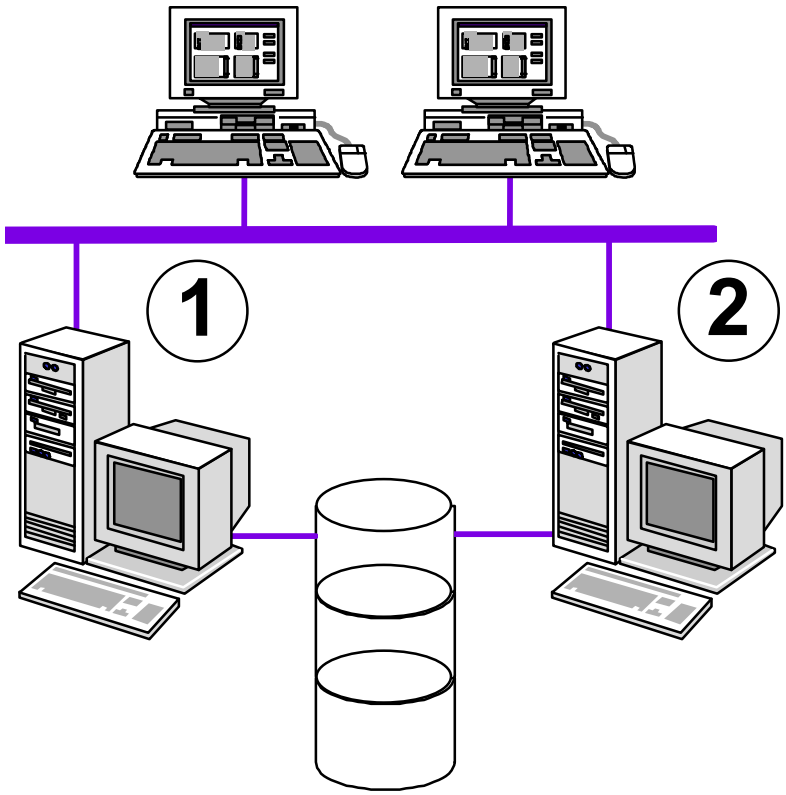
Klusterien ominaisuuksia ovat seuraavat:

- **Käytettävyys** - jos yksi palvelin kaatuu, vika eristetään ja palvelimen tehtävät siirretään toisiin palvelimiin. Käyttäjät eivät parhaimmillaan huomaa mitään vikatilanteita syntyneenkään

- **Skaalattavuus** - palvelimien lisääminen tuo lisää suorituskykyä

- **Hallittavuus** - kuormituksen tasaaminen tai palvelimien ylläpito hoidettavissa keskitetysti.

Tässä esimerkissä kaksi klusteriin kuuluvaa palvelinta jakaa samaa kiintolevyä. Jos palvelimeen **1** tulee jokin vika, prosessit siirretään palvelimeen **2**, mikä ryhtyy palvelemaan käyttäjiä. Levyjärjestelmä voi itsessään olla vikasietoinen (esimerkiksi **RAID 1** tai **RAID 5**).



Itse klusteriympäristön lisäksi myös tulee huomata järjestelmässä ajettavat **sovellukset**. Sovellusten (prosessien) kannalta on syytä huomata, että osa sovelluksista saattaa toimia **suoraan** klusteriympäristössä (*Cluster Aware Application*), osa taas ei. Esimerkiksi tietokantapalvelimen tulee osata hallita klusteriympäristön jaetun datan käsittely tai **Shared Nothing** -mallissa sen tulee osata jakaa ja käsitellä rinnakkaiset kyselyt. Lisäksi elpyminen virhetilanteista tulee käsitellä hallitusti - tavallisesti tämä toteutetaan klusterin API:en (*Application Programming Interface*) avulla.

Microsoft on tuomassa Windows NT-ympäristön klusterointiratkaisuksi **Windows NT NT Cluster Serveriä** (*Wolfpack*). Kannattaa huomata, että myös muilla valmistajilla on omia ratkaisuitaan klusterointiin Windows NT-ympäristössä, esimerkiksi:

- **NCR**, LifeKeeper, jaettu SCSI-levyjärjestelmä ja fail-over-optiot useille sovelluksille, lisäksi klusterointi palvelinlaitteistossa, **http://www.ncr.com**

- **Vinca**, Vinca Standby-Server, **http://www.vinca.com**

- **Convoy Cluster Software**, TCP/IP-palveluiden klusterointi, **http://www.valence.com**

- **Digital Equipment**, Digital Clusters for Windows NT, jaettu SCSI-levyjärjestelmä ja fail-over-optiot useille sovelluksille, **http://www.windows.digital.com**

- **Marathon Technologies**, Endurance 4000, Pentium Pro-palvelimien yhteenliittäminen, ei edellytä laitteisto- tai ohjelmistotason muutoksia, **http://www.marathontechnologies.com**

- **Hewlett-Packard**, HP High-Availability Clustering Solutions for NetServers, kaksi palvelinta ja MSCS, **http://www.hp.com/go/netserver**

- **NTServ/IS**, useiden kaksiprosessorijärjestelmien yhdistäminen - tuki MSCS:lle tulossa, **http://www.cubix.com**

- **Stratus Computer**, RADIO Cluster, sekä laitteisto- että ohjelmistotason virhetilanteista elpyminen, **http://www.stratus.com**

- **Data General**, NT Cluster-in-a-box, kaksi palvelinta ja SCSI-levyjärjestelmä, klusteriohjelmisto on **First Watch**, **http://www.dg.com** ja **http://www.veritas.com**

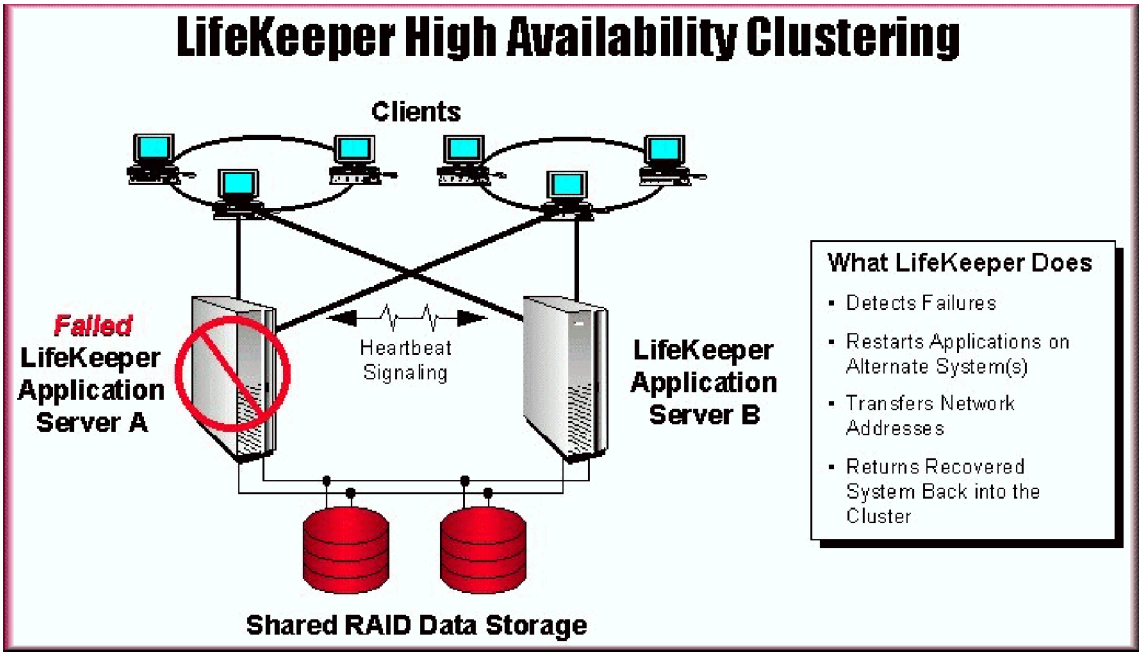
- **Octopus SASO**, täydellinen järjestelmän kopio, **http://www.octopustech.com**

- **Compaq Computer**, Recovery Server Option, ProLiant- ja ProSignia-palvelimien vikasietoisuusratkaisu, jatkossa tulee MSCS- ja ServerNet-tuki. Compaq ja Tandem julkistivat loka-

kuussa 1995 klusteriyhteistyönsä ja Compaq esitteli jo joulukuussa 1996 Wolfpackin betaversiossa SAP R/3-sovellusta. Tandem sen sijaan on esitellyt **Cluster Availability Solution** (CAS) 1.1:n, joka tuo mm. MSCS-yhteensopivan API:n. Tandemin **ServerNet**-ratkaisua tukee myös Compaq, ja nyt entistäkin enemmän, kun kesäkuussa 1997 Compaq ja Tandem yhdistyivät. Ks. **http://www.compaq.com** ja **http://www.tandem.com**.

NCR LifeKeeper

NCR esitteli LifeKeeper-ratkaisun Windows NT-ympäristöön tammikuussa 1996. LifeKeeperin idea on se, että kaikki klusterin komponentit ja palvelut ovat koko ajan käytettävissä. Tiedonsiirrossa klusterin komponenttien välillä käytetään *heartbeat*-signaalia. Kun palvelimen virhetilanne huomataan, muut klusterin palvelimet ryhtyvät jakamaan kaatuneen palvelimen jakamia resursseja. LifeKeeperissä on myös omia mekanismejaan palvelimen palauttamiseks
i takaisin klusteriin.



Seuraaviin ohjelmistoihin on saatavissa sovellustason LifeKeeper-tuki:

- Informix
- Oracle
- Sybase
- MS SQL Server
- MS Exchange
- MS LAN Manager
- TCP/IP
- Lotus Notes
- PeopleSoft
- SAP R/3.

Windows NT Cluster Server

Windows NT NT Cluster Server (MSCS, *Wolfpack*) on Microsoftin ratkaisu klusterointiin Windows NT-ympäristössä, ja se on osa syksyllä 1997 tulevaa **Windows NT 4.0 Enterprise Editionia** (*Granite*). Suunnittelutavoitteet MSCS:ssä ovat olleet:

- **Cluster-API** (*Application Programming Interface*), joka mahdollistaa sovellusten rakentamisen klusteriympäristöön

- **Nykyisten palvelinlaitteistojen tuki** - tässä saa kuitenkin olla tarkkana. MSCS edellyttää SCSI-laitteistoilta piirteitä, joita ei kaikissa SCSI-ohjaimissa ole

- **Palvelinsovellusten tuki** - esimerkiksi BackOffice-tuotteet tulevat tukemaan klusteriympäristöä

- **Käyttöönoton joustavuus** olemassaolevien Windows NT:n suojausmekanismien ja valvontatyökalujen avulla. Klusterin hallintatyökalut ovat samantyyppisiä kuin muutkin Windows NT:n työkalut.

Alkuvaiheessa ratkaisu tukee kahden palvelimen (*two-node*) vikasietoista (*fail-over*) klusteria ja seuraavassa vaiheessa tuki tulee useammille palvelimille ja kuormituksen jakamiselle. Tällöin klusterin suorituskyvyn loppuessa klusteriin voidaan lisätä esimerkiksi lisää palvelimia.

Tavallinen Windows NT Cluster Server -ympäristö sisältää ensi vaiheessa kaksi palvelinta (edellyttää sertifiointia), joilla on yhteinen SCSI-kanava esimerkiksi levy-yksikköön. Palvelimien verkkoliitäntä voi noudattaa perinteistä tapaa, vaikka Microsoft suositteleekin erillistä verkkoa klusterin palvelimien väliseen tiedonsiirtoon. Kuormituksen tasaaminen voidaan hoitaa ensi vaiheessa luomalla kaksi jakoa samaan fyysiseen resurssiin, ja määrittelemällä molemmat palvelimet toisen resurssin omistajaksi ja ohjaamalla vikatilanteessa kyseinen resurssi toiselle palvelimelle. Tämän jälkeen määritellään resurssien käyttöoikeuspolitiikka siten, että käyttäjien aiheuttama kuormitus jaetaan resurssien kesken.

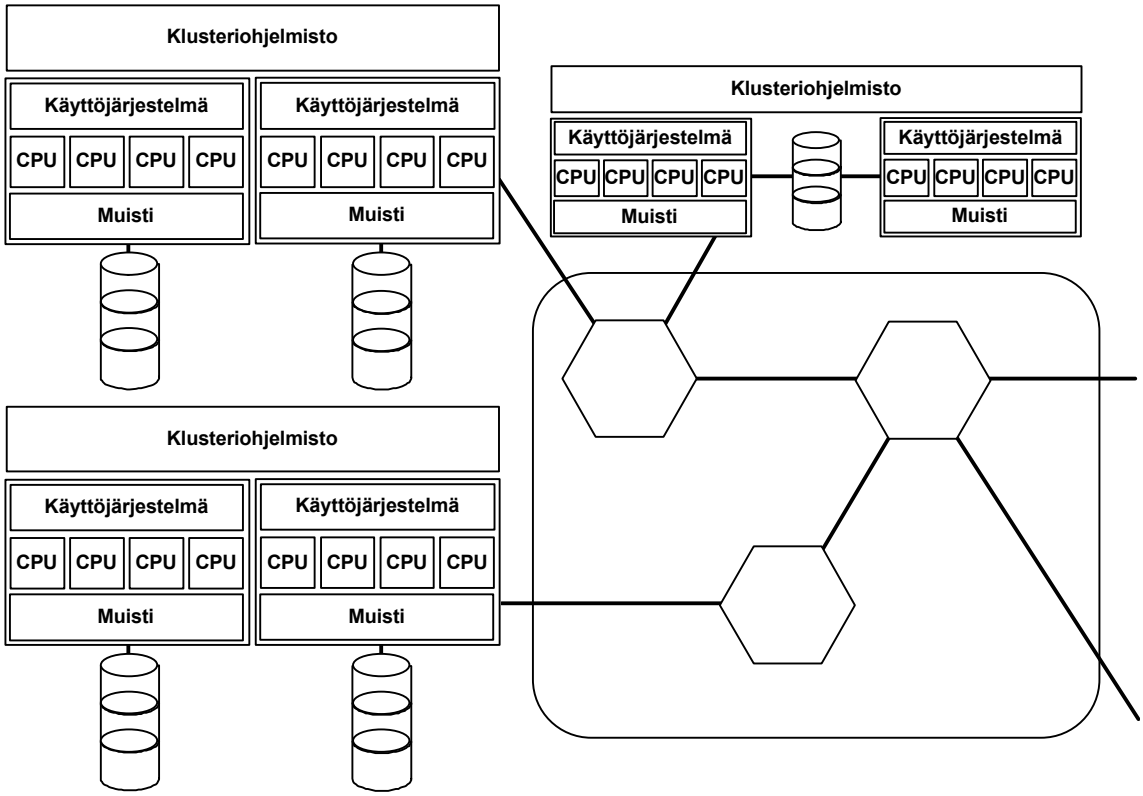
Sovellustason kuormituksen tasaus tulee rakentaa itse sovellukseen. Tähän tarkoitukseen on saatavissa **Windows NT Cluster Server Software Development Kit**.

Tandem ServerNet SAN

Klusterin komponenttien välinen luotettava ja riittävän suurikapasiteettinen tiedonsiirto LAN:in ja WAN:in avulla on nähty ongelmaksi, ja ratkaisuksi tarjotaan **SAN**:ia (*System Area Network*), joka kehitetään nimenomaan minimoimaan viivet ja nostamaan klusterin komponenttien välisen tiedonsiirron kapasiteettia. **Virtual Interface Architecture** (*VI Architecture*) on määrittely näille SAN:in komponenteille. SAN:in idea on se, että klusterin jokainen itsenäinen komponentti on käytettävissä, ja vieläpä ilman prosessorin kuormitusta. Tämä on toteutettu siten, että komponentit voivat keskustella suoraan keskenään ohittaen palvelinten prosessorit.

Konseptin tuotenimi on **ServerNet**, ja se on ollut käytettävissä Tandemin Integrity S4000-Unix-palvelimissa vuodesta 1996. Menetelmässä käyte-

tään hyväksi ASIC-pohjaista kytkintekniikkaa, ja kytkimen teho on 1,3 Gt sekunnissa. Palvelimen liitäntä hoidetaan PCI-väylän kortilla. Kytkimiä voidaan liittää toisiinsa (ks. kuva), ja näin klusteriin voidaan liittää 1000000 komponenttia. Vastaavasti klusteriin lisättävät kytkimet lisäävät järjestelmän tiedonsiirtokykyä aina 150000 gigabittiin sekunnissa. Mainittakoon, että eräs ServerNetin kehittäjistä Tandemin Cupertinon laboratoriossa on suomalaissyntyinen Henrik Åberg.

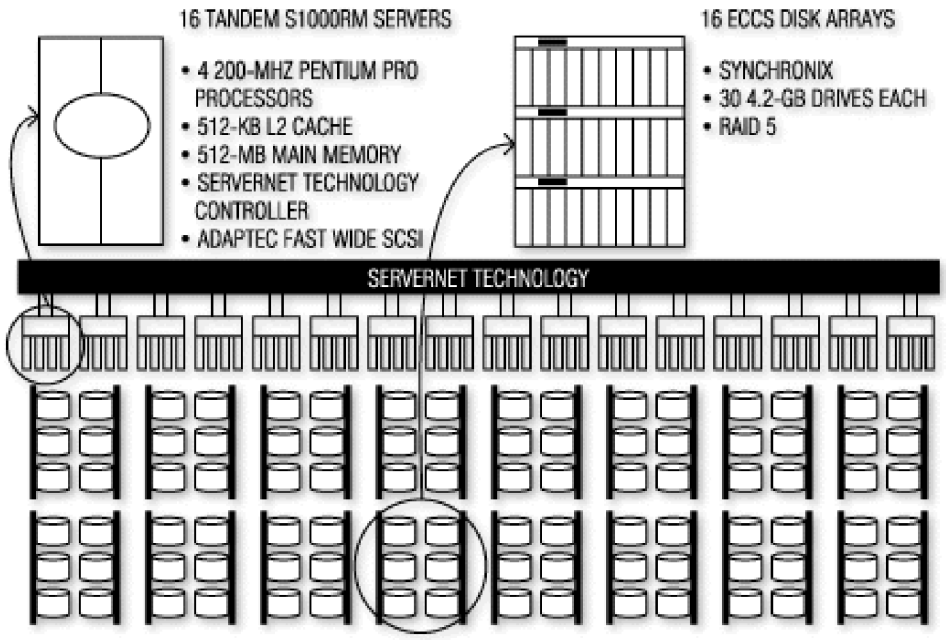


ServerNetiin voidaan kytkeä muitakin laitteita palvelimia, esimerkiksi SCSI-laitteita. Se on siis puhtaasti laitteistotason ratkaisu. Varsinaiseksi klusteriohjelmistoksi ratkaisussa tarjotaan **Windows NT NT Cluster Serveriä** (*Wolfpack*).

Lisätietoja:

- **Tandem**, **http://www.tandem.com**
- **Tandem & Microsoft**, **http://www.bizcritical.com**

Tandem esitteli ServerNetin toimintaa käytännössä Intelin *The Future of*

Business Computing-tilaisuudessa New York Cityssä 2.6.1997. Tarkoitus oli esitellä Intel-prosessorien käyttökelpoisuutta päätöksenteon tukijärjestelmässä, jonka tietokanta oli kooltaan kaksi teratavua.

Esityksessä käytetty klusteri sisälsi 16 kappaletta 4-prosessorisia (Pentium Pro/200 MHz) S1000-palvelimia. Tällöin koko klusteri käsitti 64 prosessoria ja 8 Gt keskusmuistia.). Levykapasiteettia oli 480 kpl 4,2 gigatavun kiintolevyjä, jolloin koko kapasiteetti yhteensä oli 2,016 teratavua! Varmistukset hoidetaan kahdeksalla Quantum 4700 DLT-nauhurilla.